CSS CYBER DEFENSE

Study on the use of reserve forces in military cybersecurity

A comparative study of selected countries

Zurich, April 2020

Cyber Defense Project (CDP)
Center for Security Studies (CSS), ETH Zürich

CSS
ETH Zurich

ETH zürich

Author: Marie Baezner

Additional research: Sean Cordey and Arthur Laudrain

Contact:
Center for Security Studies
Haldeneggsteig 4
ETH Zürich
CH-8092 Zürich
Switzerland
Tel.: +41 44 632 40 25
css.info@sipo.gess.ethz.ch
www.css.ethz.ch

Analysis prepared by: Center for Security Studies (CSS), ETH Zürich

ETH-CSS project management: Tim Prior, Head of the Risk and Resilience Research Group; Myriam Dunn Cavelty, Deputy Head for Research and Teaching; Andreas Wenger, Director of the CSS

Disclaimer: The opinions presented in this study exclusively reflect the authors' views.

Please cite as: Baezner, Marie (2020): CSS Cyber Defense Report: Study on the use of reserve forces in military cybersecurity, April 2020, Center for Security Studies (CSS), ETH Zürich.

Table of Contents

1 Introduction

1.1 Context and goal of the report

Globally, states have embraced digitization and are trying to shape the global technological transformation. Generally, the digital transformation has been perceived positively, delivering new opportunities and socio-economic benefits. However, digital technologies have also created new criminal and political risks for states.

Criminal and political cyberattacks have become more prominent in the media in recent years. Awareness is growing in policy circles, and many states have developed their own national cybersecurity and defense strategies. Many strategies call for the development or reinforcement of defensive cybersecurity capabilities[1] (including military cybersecurity capabilities). In building these cyber capabilities, states are confronted with many challenges that are not solely technical in nature but also concern human resources. Indeed, (ISC)² (2018) estimated that the cybersecurity workforce gap was close to three million in 2018 worldwide. Globally, both private-sector companies and state institutions struggle to find skilled personnel in cybersecurity. Both sectors also compete against one another to attract the personnel that is available. In this competition, public institutions and especially the armed forces are penalized by their limited resources and frequently inflexible structures and hierarchies. However, reserve forces (including conscript armies), being a military service sitting in between active-duty military service and civilian life, seem particularly well-suited for cybersecurity military tasks and appear to be one solution to attract qualified personnel (Lomsky-Feder et al., 2008). While armed forces are seriously disadvantaged on the labor market compared to the private sector, reserves offer a solution for hiring qualified personnel interested and/or trained in cybersecurity who may not have joined the military without this option. This solution also benefits reservists through the possibility to gain experience and/or training that can also benefit their civilian careers. Therefore, cyber reserves present three significant advantages for armed forces:

- They are less costly than all-volunteer forces.
- They help to close the workforce gap.
- They help to develop closer ties between civil society and the armed forces.

Based on these observations, this study aims to answer the following questions:

- What are the different types of cyber reserves? How are they structured? How are they organized?
- What are the advantages of having cyber reserves?
- What are the challenges that states face when setting up or having a cyber reserve force? How can these challenges be faced?

To answer these questions, this report examines the cyber reserve forces of Estonia, Finland, France, Israel, Switzerland, and the United States. These six countries constitute a sufficiently diverse sample group to represent six different types of reserve forces in Western states. In other words, each of these reserves is different and represents a particular type of cyber reserve in a specific setting.

1.2 Summary of findings

There are three primary findings from the comparison study done for this report. The first finding relates to the importance of **context** in the development of cyber reserve forces. There is no single solution that fits all states when it comes to the establishment of cyber reserves. Consequently, states cannot simply copy a reserve system and apply it unchanged to their situation. The organization and structure of cyber reserves necessarily depends on states' resources, strategic culture, political institutions and political context, among others.

The second finding concerns the positive impact the use of cyber reserve forces has in **countering the workforce shortage** in the armed forces. The fact that cyber reserve force personnel is employed part-time by the armed forces seems to be appealing to cybersecurity specialists. Consequently, cyber reserves have almost no issue recruiting cybersecurity specialists.

Third, most case studies show that cyber reserve forces are **works in progress.** States proceed by trial and error in developing their cyber reserves, and they sometimes suffer setbacks.

1.3 Methodology

The research for this study consisted primarily of desktop research. The first step was to gather information on each state's reserve forces employed in cybersecurity. This information was collated in a comparison table[2] that served to identify gaps. The open-source literature drawn on in the research included both primary sources (e.g. official reports and documents produced by armed forces for

1 Offensive cybersecurity capabilities tend to be less prominent in national cybersecurity strategies, but are also taken into account.

2 The comparison table can be found in Annex 1.

recruitment purposes) and secondary sources such as media articles, studies from think tanks and private institutions, and academic articles.

Once relevant gaps had been identified, research proceeded by reaching out to field experts in these six countries for interviews. Interviewees received questions in advance, and interviews were conducted through semi-structured telephone or Skype conversations.

1.4 Disclaimer

The research for this study was based on open-source material, which can bring some challenges. A great deal of information relating to the armed forces and, more specifically, to cybersecurity is classified and therefore not available to the public. As a result, it is difficult to build a complete dataset about the use of reserve forces in cybersecurity. This research tried to overcome this issue by conducting interviews, but gaps still remain. Also, some countries are more transparent about their military practices than others, which resulted in a certain disequilibrium of information, as some states' profiles are less detailed than others. However, this imbalance does not necessarily mean that these countries do less with their reserve forces in cybersecurity; it merely indicates that the sources available for the relevant countries were less comprehensive than for others. Finally, this study focuses on six case studies, but other states also use their reserve forces in cyberdefense missions. However, these cases were not included because of a lack of information, or the cases were judged to be of limited relevance for this study. As a result, the cases presented in this research may not be fully representative, but they are sufficiently relevant and inclusive to build a comprehensive analysis.

1.5 Overview

Chapter 2 introduces the subject of cyber reserves and lays a sound basis for the study by defining cyber reserves within the framework of current research. The chapter describes the different types of cyber reserve forces available and their particularities before briefly examining the advantages of developing a cyber reserve force.

Chapter 3 profiles the cyber reserve forces of Estonia, Finland, France, Israel, Switzerland, and the US. The chapter describes the process reserve members go through from the time of their recruitment, including relevant training programs and reserve members' roles and responsibilities. The country profiles in this chapter also look more generally at the size of cyber reserve forces, the organization of military service for reserve forces, reserve members' potential links with the private sector, and whether cyber reservists stay in contact after the end of their military service.

Chapter 4 presents an integrated overview of the six countries' cyber reserve forces based on the elements examined in Chapter 3.

In Chapter 5, the report focuses on the challenges that armed forces may encounter in the development of their cyber reserve forces, and how some states overcome these challenges. This chapter examines seven main issues:

- Difficulties recruiting the right individuals
- How to integrate cyber reserves into the national security apparatus
- Difficulties organizing training programs
- Security risks
- Cost-efficiency of cyber reserves
- Managing the availability of reservists
- How to win and maintain the loyalty of reservists

Finally, Chapter 6 summarizes the core findings of the report.

2 What are cyber reserves?

This report aims to shed light on the use of reserve forces in cybersecurity by examining relevant practices in six states. In order to look at the various reserve forces, the report first needs to set out precisely what is understood by the term "cyber reserve". This chapter clarifies the terminology used in the report, including specifically the terms "reserves", "cyber reserves", "cyber reserve forces" and "cyber reservists".

The study bases its definition of "cyber reserve" on three criteria common to all of the six case studies investigated in order to establish a broadly applicable definition. Reserves:

- Form part of the state's national security apparatus
- Are a component of the state's military forces that supports active-duty military personnel and/or constitutes additional forces to such personnel
- Has personnel whose primary source of income is not derived from their military activities

For the purposes of this study, conscription-based armed forces consequently come within the meaning of reserve forces as defined in this report. Indeed, while conscripts can be recognized as active-duty forces during their mandatory military service, they are also organized similarly to reserve forces at the same time. Conscripts are trained for tasks similar to active-duty personnel and also support permanent personnel. They go back to civilian life after their basic training, and in some conscription models they continue their military service through yearly refresher trainings. In this form of conscription, conscripts' primary source of income, apart from the period of basic military training (several months), is not derived from their military activities. Therefore, conscription-based armed forces meet all three of the aforementioned criteria for inclusion in this study as reserve forces.

Moreover, paramilitary and military institutions that employ volunteers and are included in and/or collaborate with an organization of the armed forces can also be recognized as reserve forces in the context of this study. Indeed, these all-volunteer military and paramilitary organizations are part of national security apparatuses and support active-duty personnel in the event of war and/or emergency. Furthermore, members of the reserve component of these all-volunteer armed forces and paramilitary organizations are by definition volunteers, but, unlike active-duty personnel, their activity within these organizations is not their primary source of revenue. For these reasons, volunteer military and paramilitary organizations are also regarded as reserve forces in this study.

2.1 Definition of cyber reserves

Cyber reserves are defined as reserve forces used in the cyber domain. By extension, cyber reserves are, therefore, part of a state's national apparatus and forces. In these reserves, the personnel are not active-duty military staff but form a part-time military or voluntary workforce tasked with cybersecurity duties for the armed forces (or paramilitary forces). Cyber reserve personnel may often work as cybersecurity or IT specialists in their civilian jobs and may be using their civilian experience and skills in the field for their military or voluntary missions.

Types of cyber reserves	Case study
Conscription with yearly refresher training	Finland, Israel and Switzerland
Voluntary paramilitary institution	Estonia
All-volunteer national guard	France and the US
All-volunteer reserve force	USA

Table 1: Different types of cyber reserves

2.2 Terminology used in this report

The variety of cases studied in this research caused certain terminological challenges. Therefore, to avoid confusion, the terminology employed in this report needs to be clarified and consistent. The six case studies in the report examine four types of armed forces reserves: conscription-based, paramilitary, national guard and reserve forces. It should be noted that some armed forces differentiate between active-duty and reserve personnel, with the latter consisting of former active-duty personnel. To ensure clarity and consistency throughout the report, the word "reserve" relates to all four forms of the aforementioned reserves. The word "reservist" relates not solely to former active-duty personnel but also to any military or paramilitary personnel employed part-time in one of the aforementioned four types of reserves. The term "reservist" is therefore used to describe conscripts, members of a paramilitary force, members of a national guard and reserve members in this report. Furthermore, the terms "cyber reserves" and cyber reserve forces" are employed interchangeably in this report without any distinction.

2.3 Advantages of reserves

Reserves in general present advantages for states, and cyber reserves can therefore be expected to deliver the same benefits by extension. Cyber reserves constitute one of several conceivable forms of organizing national

cyberdefense. The use of reservists in cybersecurity presents significant advantages compared to exclusively employing professional cybersecurity troops, namely lower costs, closure of the personnel gap in the cyberdefense workforce through more appealing working conditions, and the establishment of closer ties between the armed forces and civil society.

Cost savings

Having a cyber reserve force allows armed forces to save on costs on personnel and training. In general, reserve forces cost less than professional forces or outsourcing. Reservists are only in service for a limited period of time, and the armed forces therefore do not have to pay them full-time wages (Bauer et al., 2012; Goodwill-management, 2017; Poutvaara and Wagener, 2007). This is a good way for armed forces to build up a large pool of cyber experts at a lower cost than with a full-time staff of experts. To employ full-time staff is also more complicated for armed forces, as they would need to bring salaries in line with the private sector in order to attract candidates.

With some forms of cyber reserve forces, armed forces can also save on recruiting and training costs. This is particularly true for cyber reserves focused on recruiting cyber experts with existing prior knowledge and experience in cybersecurity (e.g. France and Estonia). These reserves do not need to actively look for talents through headhunters. They also do not need to organize and conduct extensive foundational training, as it is sufficient for them to provide training to bring experts up to date for their task(s).

Closure of the personnel gap

The creation of cyber reserves helps armed forces to close the workforce gap in cybersecurity. Finding and hiring enough qualified personnel constitutes a serious challenge for armed forces in cybersecurity, as armed forces compete directly with other government agencies and the private sector in this market (Libicki et al., 2014; Porche, 2017). Providing cybersecurity experts with the option to join a cyber reserve allows them to join the armed forces on more flexible terms. Some experts may be interested in joining the regular military but are deterred by low salaries or concerns regarding potential restrictions in military life. These experts may find it more appealing to join a cyber reserve that is only deployed for a few weeks every year.

Closer ties between the armed forces and civil society

Reservists have a primary job from which they derive their revenue, i.e. their civilian job, and a secondary job from which they only get a compensation, i.e. their military job. This duality puts reservists in an advantageous position that also benefits both of their employers. Reservists can learn from both their jobs and transfer their knowledge and expertise from one job to the other. Lomsky-Feder et al (2008), who based their research on Israeli reservists, argued that Israeli reservists can be seen as bridging the two worlds of the military and civil society. They assert that reservists can learn from and enrich both worlds with their experiences and knowledge from the respective other (Lomsky-Feder et al., 2008).

Consequently, having reservists in cybersecurity increases public-private collaboration. Reservists coming from cybersecurity firms may share their knowledge and experience from their civilian workplaces with the armed forces and vice versa. This practice creates greater awareness in the armed forces of developments in the private sector and vice versa, with both domains benefiting from such exchanges.

Finally, cyber reserves serve as networking platforms for cyber reservists. They meet other cybersecurity experts, get to know them and work with them during their reservist duty. These ties among reservists become useful for reservists themselves (e.g. for recruitment or job seeking) and for the cybersecurity sector. Reservists exchange experiences and knowledge, but they also become personal points of contact for others. In case of an emergency, for example if a reservist's company falls victim to a cyberattack and the reservist knows that another reservist's company suffered a similar attack, the former could get in touch with the latter to get advice on how to solve the issue.

3 Profiles of six cyber reserves

This study examines six countries that have military or paramilitary reserves and use them in (offensive and/or defensive) cyber operations. These countries are Estonia, France, Finland, Israel, Switzerland and the US. The countries examined in this report were selected not only for their use of reserve forces but also for the variety of these forces. The analysis of the selected countries bases this research on a broad range of Western democracies with all-volunteer as well as conscription-based armed forces, with both military and paramilitary armed forces involved in cyber operations, with large and smaller armed forces, and with members and non-members of NATO[3] and/or the European Union (EU) and neutral countries. Given the diversity arising from the comprehensive selection of case studies, this chapter aims to describe this diversity by examining how these countries organize their cyber reserve forces. This description then serves as the starting point for Chapters 4 and 5, which analyze the practices implemented and challenges faced by these states with regard to their cyber reserves.

The description of each state's cyber reserve is structured according to the following six aspects:[4]

1. **Recruitment process and training:** This segment describes how a volunteer or conscript goes from civilian to cyber reservist. It looks at the recruitment criteria for cyber reserve positions and the training required once accepted.
2. **Roles, tasks and responsibilities of cyber reservists in the cyber reserve:** This segment sets out the possible roles that cyber reservists can have within the armed forces and their associated tasks and responsibilities.
3. **Number of cyber reservists:** This segment attempts to determine the size of each cyber reserve. Relevant numbers need to be put into perspective, as published numbers may sometimes reflect political and signaling purposes rather than reality.
4. **Organization of the service: Length of military service and refresher trainings:** This segment describes how the duty of cyber reservists is organized, whether they have mandatory refresher trainings every year or whether their training is organized differently. The study also looks at how long cyber reservists need to serve.
5. **Links between the armed forces and the private sector regarding the reserve:** This segment looks at whether the private sector has partnerships with the armed forces regarding cyber reserves (e.g. in training, planning of reserve duty, internships, employment, etc.).
6. **Post-reserve duty (career and keeping ties with the armed forces):** This segment examines whether former cyber reservists stay in touch with each other and/or with the armed forces through organized or informal structures. Additionally, this part tries to determine if former cyber reservists pursue careers in cybersecurity.

As this research is based on open-source materials and interviews, the amount of information available for each state is unevenly distributed. Some states are more transparent than others about their reserve force activities, structure and organization. This imbalance in the volume and descriptiveness of the available information does not reflect the size or capabilities of cyber reserves but is merely indicative of the amount of data that could be found and processed.

The states are listed and examined in alphabetical order, and their order does not indicate any preference or ranking.

3 Abbreviations are listed in Section 10.

4 A table in Annex 1 summarizes the cyber reserve practices of all six states.

3.1 Estonia

Estonia is a unitary parliamentary republic which regained its independence in 1991 after the fall of the Soviet Union. It is considered to be one of the world's most highly digitalized countries. Estonia has been a member of the EU and NATO since 2004. Estonia has hosted the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn since 2007.

Estonia has both a conscription-based army and a paramilitary force, the Estonian Defence League (EDL), which serves to support to civilian and military authorities in times of peace and crisis. The strong Estonian military with approximately 6,600 active-duty personnel and 12,000 reservists is supplemented by 25,000 paramilitary troops (International Institute for Strategic Studies, 2018; Ottis, 2019).

Estonia was in the international spotlight in 2007 when cyberattacks paralyzed the websites of banks and state institutions. These cyberattacks were attributed to Russian nationalist groups and were most likely triggered by Estonia's decision to relocate a Soviet-era memorial. The cyberattacks caused the military in Western states to consider the importance of cyberspace in conflicts, and NATO established the CCDCOE in Tallinn in the wake of these attacks.

In Estonia, the EDL is likely the largest unit of cybersecurity reservists. Therefore, this section limits its discussion to the EDL Cyber Defence Unit (EDL CDU) and does not consider the part played by the conscription-based military in cybersecurity. Following the 2007 cyberattacks, there was a bottom-up initiative of people wishing to volunteer in cybersecurity without wanting to join the military. This initiative was followed through with the establishment of the EDL CDU in 2009, which was formally recognized by the Estonian authorities in 2011 (Cardash et al., 2013; Ottis, 2019).

Recruitment process and training

Joining the EDL is voluntary and open to all Estonian citizens. To join the EDL CDU, volunteers need to:

- Pay a €12 annual membership fee
- Be at least 18 years old
- Be loyal to the republic of Estonia
- Recognize the independence and constitutional order of Estonia
- Pass a background check
- Have knowledge, skills or interests relevant to cybersecurity
- Present two reference letters from current members of the EDL CDU[5]

Volunteers wishing to join the EDL CDU do not need to have technical skills, as non-technical profiles are also sought, and volunteers do not need to have served in the Estonian military. The latter criterion is considered important for attracting people unable to join the Estonian military who still want to serve their country (Estonian Defence League, 2019a; Kaska et al., 2013).

EDL CDU volunteers can attend general cybersecurity training to update their knowledge and skills, but specialist training in certain domains of cybersecurity is left to individuals. Volunteers organize more or fewer trainings and exercises, depending on their units' level of practice. In addition, refreshers are regularly organized to keep volunteers up to date (Ottis, 2019).

Roles, tasks and responsibilities of reservists enrolled in cyber reserve

The role of the EDL CDU is to raise cybersecurity awareness within society, share knowledge on cyberthreats among IT specialists, and support crisis management mechanisms by protecting critical infrastructures (Estonian Defence League, 2019b). There are no official or predefined roles in the EDL CDU, but volunteers joining the unit can come from the following backgrounds:

- IT specialists from national critical infrastructures
- Patriotic individuals with technical knowledge and skills
- Specialists in fields other than cybersecurity (law, social sciences, economics) with an interest in cyber issues (Estonian Defence League, 2019a, 2019b; Ottis, 2019)

All EDL CDU members are tasked with autonomously pursuing initial and further professional training and ensuring the security of the population during peacetime. For these purposes, members of the EDL CDU participate in activities to improve their knowledge, skills and experience and raise general awareness among the broader population. The EDL CDU also regularly organizes seminars, information-sharing and training events. Members can also participate in exercises such as national security exercises or NATO exercises like Locked Shields.

The EDL CDU also supports private and public actors in cybersecurity. Members of the EDL CDU offer consultations, technical security solutions and expert skills. Members have been involved in installing malware screening tools on school computers and security testing the Estonian e-voting system, among others.

As a supplementary task, the EDL CDU offers assistance in cases of emergency and crisis, supporting authorities in cybersecurity. Any private or public entity can request support from the EDL CDU via the State Information Systems Authority (SISA) (Kaska et al., 2013).

5 Candidates who do not have reference letters may be accepted for a "candidacy period" of up to one year, during which they can participate in EDL CDU activities but do not have the rights and obligations that members have (Kaska et al., 2013).

Numbers of cyber reservists

There are no official numbers on volunteers in the EDL CDU.

Organization of the service: Length of military service and refresher trainings

Members of the EDL CDU are volunteers who stay with the organization until they leave it or are expelled. As EDL CDU members are volunteers, they are under no legal obligation to participate in activities. However, they have a moral obligation to participate, and if they choose not to participate, they are required to justify their absence, although they are not penalized. EDL CDU members do not get paid a salary for their work, but they can receive some compensation. In cases of emergency, members can be engaged for a maximum, non-renewable period of 30 days[6] (Kaska et al., 2013).

EDL trainings in general but also in the EDL CDU are organized in *ad hoc* settings depending on the respective unit and its volunteers. Some units or volunteers are more involved and organize more training sessions and exercises than others (Ottis, 2019).

Links between the armed forces and the private sector regarding the reserve

The EDL CDU enjoys a good reputation among Estonian companies and is used as a networking platform by the private sector to informally contact IT specialists from other firms. Employers sometimes suggest to their employees that they join the EDL CDU for this particular purpose (Ruiz, 2018).

The EDL CDU also has an international partnership with the 175th Wing Cyber Operations Group of the Maryland Air National Guard. Both units participate in joint exercises and exchange experiences and knowledge (Rauschenberg, 2018).

Post-reserve duty (career and keeping ties with the armed forces)

Some members of the EDL CDU stay in contact with each other outside the trainings, albeit informally (Ottis, 2019).

Estonia

Estonian Defence League Cyber Defence Unit

Recruitment	Voluntary
Training	No mandatory training but can attend
Enrolment	Part of EDL CDU regular training and exercises

Figure 1: Journey of a member of the EDL CDU

6 Except in the case of a national emergency, where this time limit does not apply.

3.2 Finland

Finland is a neutral state and a unitary parliamentary republic with conscription-based armed forces. Finland joined the EU in 1995, is part of the NATO Partnership for Peace (PfP) and hosts the joint EU-NATO Centre for Countering Hybrid Threats.

Finland's armed forces are primarily composed of conscripts and reservists. The armed forces include 33,500 active-duty personnel (including both conscripts completing their initial military training and professional military personnel) and approximately 230,000 reservists who can be mobilized in time of war. Of these, approximately 18,000 are called up for refresher trainings annually, while others have the possibility to participate in voluntary exercises (Prime Minister's Office, 2017; The Finnish Defence Forces, 2017, 2015). Finland's 2019 military budget was €3.1 billion, but the country plans to increase military spending in the coming years (Ministry of Defence, 2019; Prime Minister's Office, 2017).

Within the Finnish Defence Forces (FDF), the C5 Agency in the Defence Command C5 Division is responsible for military cyberdefense. Its role and focus are to promote situational awareness in cyberspace, plan and conduct defensive cyber operations, and protect and monitor FDF networks (Prime Minister's Office, 2017). However, a new intelligence law adopted in 2019 will enable the FDF cyber unit to also conduct offensive cyber operations (Ministry of Interior, 2019). Conscripts have served with the C5 Agency as cyber specialists since the fall of 2015. Each military branch command also has its own cyber unit composed of permanent military personnel (Nokelainen, 2019). The FDF is currently undergoing reforms including plans to create a centralized cyber command (The Security Committee, 2016).

Recruitment process and training

All Finnish male citizens must complete compulsory military service between the ages of 18 and 60; female citizens can apply for voluntary military service.[7] At the age of 18, Finnish men attend a call-up where they are informed when and where they will complete their military service.[8] Initial military service takes 165, 255 or 347 days, depending on the conscript's function in the FDF. After this initial military service, conscripts join the reserve (The Finnish Defence Forces, 2019, n.d.).

Basic military training lasts eight weeks and is the same for all branches of the military. During basic training, conscripts can choose to specialize in cybersecurity by applying online, on their own initiative, to be assigned to "special duties" in information technologies before the end of the third week of basic training.[9] During the remaining time in basic military training, cyber specialist candidates are then tested on their skills in areas such as network technology, programming, operating systems, applications, or software development. If they pass these tests, they continue on to cyber specialist training (Nokelainen, 2019; The Finnish Defence Forces, 2019). Specialist training is five and a half months for soldiers and 11 months for officers. Military service for cybersecurity specialists lasts a total of 255 days for soldiers. Candidates with dual nationality cannot be accepted for cyber specialist training, as it involves access to sensitive data (Cederberg, 2019). Candidates also need to demonstrate high motivation to work in an intense work environment and face challenging tasks, and they must be able to commit to continuing education. Training to become a cyber specialist comprises penetration testing, communication and blue team vs. red team exercises. Conscripts also have the option to participate in international exercises such as Locked Shields (Defence Forces C5 Agency, 2019; The Finnish Defence Forces, 2019, n.d.).

Training aims to build work experience and is heavily focused on practical training and exercises. It consists of practicing in cyber range or pen testing exercises or working directly with permanent military personnel. Conscripts specializing in cybersecurity go through the entire training together as a group and remain in the same group for refresher trainings until the end of their compulsory military service. The goal is to develop them as a team and have them work and develop as a unit (Cederberg, 2019; Nokelainen, 2019; The Finnish Defence Forces, n.d.).

Roles, tasks and responsibilities of reservists enrolled in cyber reserve

There is only a single cyber-related role open to Finnish conscripts with an interest in cybersecurity, namely that of cyber specialist. However, tasks within this role vary and consist of:

- Blue team vs. red team exercises
- Building and testing systems
- Defending FDF networks
- Programming projects
- Building situational awareness

After their task-specific training, most cyber specialists are integrated into the FDF cyber unit within the C5 Agency, while a select few specialists may be sent to military branch commands to work with permanent military

7 Female members of the FDF constitute approximately 5% of the FDF (Cederberg, 2019).

8 Finnish conscripts can also choose to complete non-military service over a period of 347 days (The Finnish Defence Forces, n.d.).

9 Officer candidates can also apply to be assigned to "special duties" in cybersecurity during their leadership training (The Finnish Defence Forces, 2019).

personnel[10] (Nokelainen, 2019; The Finnish Defence Forces, n.d.).

Numbers of cyber reservists

The C5 Agency is composed of 400 personnel, predominantly civilians (The Finnish Defence Forces, n.d.). The C5 Agency has a cyberdefense unit, which employs conscripts during their military service. The numbers of reserve and active cyber specialists are confidential (Nokelainen, 2019), making it difficult to evaluate the size of specialist cyber units.

In times of emergency, reservists from the reserve can be mobilized to support civilian personnel (The Finnish Defence Forces, 2019). However, at this stage, civilian cybersecurity experts can be mobilized in the wartime forces.[11] These experts work in cybersecurity in their civilian life and have been hand-picked by the FDF, but they may not have done their military service in a cyber unit. In the long-term, these professionals may be replaced by current conscripts and reservists trained as cyber specialists (Cederberg, 2019; Nokelainen, 2019).

Organization of the service: Length of military service and refresher trainings

Once conscripts have finished their 255 or 347 days of active military service, they are assigned to the reserve until they reach the age of 50 (60 for officers and non-commissioned officers (NCOs)). Throughout their reserve period, reservists are required to attend refresher trainings for a total of 80 to 150 days (200 for officers and NCOs). Refresher trainings usually last five to six days (The Finnish Defence Forces, 2019) and take place irregularly every one to five years (The Finnish Defence Forces, 2017). However, given that cybersecurity is a rapidly evolving field, cyber reserve units undergo refresher trainings more frequently than other units, in other words, every two to three years (Cederberg, 2019; Nokelainen, 2019). These refresher trainings consist of exercises such as red against blue teams or involve participation in international exercises such as Locked Shields (Nokelainen, 2019). Like other units, cyber units can also participate in voluntary exercises organized by the National Defence Training Association of Finland (a public association managed by the Ministry of Defense), or the FDF (The Finnish Defence Forces, 2017).

Links between the armed forces and the private sector regarding the reserve

The FDF maintains ties and regular exchanges with universities and the private sector. Finnish universities play a significant role in providing advanced technical training to civilian personnel of the C5 agency and FDF officers and in developing tools and platforms for training and exercises. The University of Jyväskylä, for example, makes its cyber range available to the FDF for training sessions (Nokelainen, 2019). Universities also collaborate with the FDF within the framework of whole-society exercises, but these exercises are not specifically focused on cyberdefense (Cederberg, 2019).

Because of the regular refresher trainings, cyber specialists move back and forth between the FDF and their regular jobs and thus serve as links between the two domains. Furthermore, the hand-picked cybersecurity experts involved in the reserve forces contribute to the exchange of experiences and knowledge with the FDF (Cederberg, 2019).

Post-reserve duty (career and keeping ties with the armed forces)

At the moment, there is no association for current or former FDF cyber reservists, but there are plans to establish one. Until then, reservists are able to participate in events and trainings of the National Defence Training Association; however, this association is open to any reservists and not only cyber reservists (Nokelainen, 2019).

10 It is planned to have more cyber specialists dispatched to military branch commands once the C5 Agency cyber specialist units are large enough (Nokelainen, 2019).

11 Positions in the wartime forces must always be filled so that they are available in times of crisis or emergency.

Finland

Finnish Defence Forces

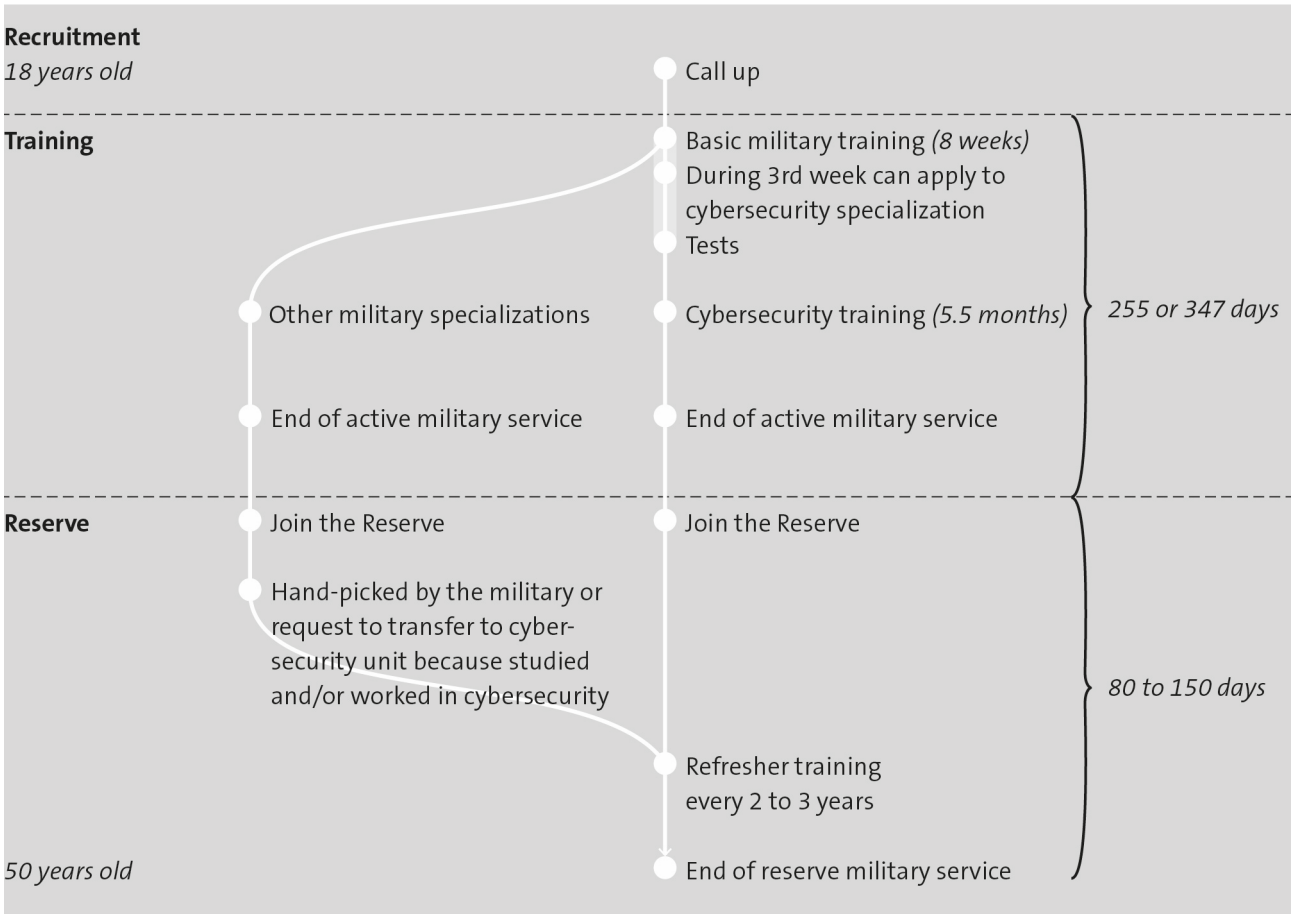

Figure 2: Possible journeys of an FDF cyber specialist

3.3 France

France is a semi-presidential republic and a founding member of the EU and NATO. It holds a permanent seat on the UN Security Council. Furthermore, France possesses a nuclear arsenal under the terms of the Non-Proliferation Treaty (NPF) and conducts military operations abroad.

The French authorities suspended mandatory conscription in 1996, making the French armed forces an all-volunteer force. The French armed forces count 270,000 personnel (204,000 active-duty and 36,300 reserve[12] personnel) (Délégation à l'information et à la communication de la défense, 2018a). France's 2019 military budget was €35.9 billion, representing 1.82% of the French GDP, but the budget is scheduled to increase to reach €44 billion in 2023. Between 2019 and 2025, the cyberdefense budget will reach €1.6 billion. In 2019, 73% of the hiring effort of the Ministry of the Armed Forces related to intelligence and cyberdefense positions (Délégation à l'information et à la communication de la défense, 2018b).

The Ministry of the Armed Forces is in charge of both offensive and defensive military cyber operations via the Cyber Command (COMCYBER) and the Directorate-General for External Security (DGSE), the external intelligence agency. COMCYBER is staffed by approximately 100 personnel primarily located in Paris (Lesellier de Chezelles, 2019). However, each military branch of the armed forces and ministerial service is required by ministerial order to have its own Security Operations Center (SOC) and to operate its own defensive cyber operations (Délégation à l'information et à la communication de la défense, 2019).

France's reserve forces consist of two types of reserves: a volunteer National Guard and an availability reserve. The first type of reserve consists of French citizens volunteering to serve part-time to support the armed forces, the National Gendarmerie or the National Police. The National Guard was established as recently as in October 2016[13] (Ministère de l'Intérieur and Ministère de la Défense, 2016). The majority of reservists involved in cyber operations come from this type of reserve. The second type of reserve is composed of former active-duty military personnel who left active duty but are required to remain in a reservist status until the end of their military career. This type of reserve is only activated in case of emergency and is not covered by the scope of this study (*Code de la défense – Article L2171-1,* 2011).

Recruitment process and training

The French cyber reserve is composed of two elements: the operational reserve and the citizen reserve.[14] Reservists in the former are paid volunteers with military status. They wear uniform, are paid according to rank and are protected by the Geneva Convention. The latter is composed of unpaid volunteers with the status of public servants.

Candidates for both cyber reserves can apply by sending their CVs and a cover letter to the *Centre de Réserve et de Préparation Opérationnelle de Cyberdéfense* (CRPOC), the center in charge of the recruitment and training of reserves for COMCYBER. Both reserves have the same set of recruiting requirements. Candidates must:

- Be French citizens and residents
- Be older than 17
- Have attended the National Service, Defense and Citizenship Day, or have been exempted
- Be clear of criminal charges or any prohibition to become public servants

In addition to the above requirements, candidates for the operational reserve must go through medical examinations, pass security clearance and complete a telephone interview. The recruitment process can take up to nine months (COMCYBER official 2, 2019).

Following recruitment, operational reservists are required to attend integration days (usually two to five days) consisting of short basic military training. Later during the same year, operational reservists attend a "cybercamp" lasting several weeks, in which they perform tasks in teams, receive further military training and are tested on their cybersecurity knowledge and abilities (COMCYBER official 2, 2019). Operational reservists are encouraged to participate in national and multinational cyber exercises (e.g. DEFNET, France's national cyber exercise, and Locked Shields, the NATO cyber exercise) (Ministère de la Défense, 2016).

A continuing education program in cybersecurity is currently being developed. This program will primarily target military professionals working in cybersecurity, but may also be opened to reservists (Durand, 2019). Furthermore, since May 2017, French universities have been

12 In this sentence, the word "reserve" is defined in the sense of former active-duty personnel.

13 The cyberdefense citizens' reserve was created in 2012 (Telecom Sud-Paris, 2016).

14 Until June 2018, there was a third element in the cyber reserve: the operational citizens' reserve. These reservists were a pool of experts who would change their reservist status from citizen reservist to operational reservist in times of emergency. Their role was to support permanent employees by performing basic network and system recovery (Gouvernement.fr, n.d.). In June 2018, the Executive Committee of the military reserve evaluated that the procedure for changing their status from operational citizen reservists to operational reservists was too complicated and inefficient. The procedure required to change the status involved compulsory medical examinations and security clearances as for operational reservists. This procedure proved to be too long and burdensome in practice. Additionally, the French armed forces encountered difficulties in managing a large number of operational citizen reservists. Therefore, the Executive Committee of the military reserve decided to stop the recruitment of operational citizen reservists and initiated a process to transfer those already recruited to the operational reserve. As a result, since June 2018, new recruitments have only focused on operational reserve needs (COMCYBER official 2, 2019; Lesellier de Chezelles, 2019).

able to grant European Credit Transfer System (ECTS) equivalencies for skills and experience acquired during reserve training (Ministère de l'Intérieur and Ministère de la Défense, 2016).

Citizen reservists do not receive any specific military or cybersecurity training for their role in the reserve (COMCYBER official 2, 2019).

Roles, tasks and responsibilities of reservists enrolled in cyber reserve

Operational reservists are assigned different roles depending on their civilian profiles. These roles are outlined in Table 2 together with their respective civilian profiles, required skills and responsibilities. As can be seen, they primarily support permanent employees.

COMCYBER is in charge of allocating operational reservists in the armed forces. A military branch or unit can request a certain number of reservists with specific skills, and COMCYBER will then allocate these to the branch or unit depending on reservists' skills and locations (COMCYBER official 2, 2019). The following units are able to request operational reservists:

- All three branches of the military (Army, Navy and Air Force) for their SOC
- The *807ème Compagnie de Transmission*[15] (in charge of cyberdefense and electronic warfare) in Rennes.

Operational reserves can work on military networks but also on the Ministry of Interior's networks if specifically requested to do so by the Ministry, or on the networks of other ministries or critical infrastructures upon request by the National Cybersecurity Agency of France (ANSSI) (Délégation à l'information et à la communication de la défense, 2018c).

The citizen reservists' role is primarily to raise awareness about cybersecurity issues in France and to strengthen the link between civil society and the armed forces (Gouvernement.fr, n.d.; Thierry, 2018). The citizen cyber reserve is divided into six groups, each in charge of a specific subject area liaising with the respective stakeholders:

- Group on elected representatives and journalists, focusing on the development of a culture of cyberdefense within society
- Group on youth, focusing on students and young professionals
- Group on the evolution of citizen engagement, focusing on the evolution of the cyberdefense reserve
- Group on think tanks and strategic thinking, focusing on technological innovations at universities and laboratories and strategic thinking in think tanks to map research on cyberdefense in France
- Group on small and medium-sized enterprises (SMEs) and small and medium-sized industries (SMIs), focusing on raising awareness of cybersecurity and cyberdefense issues among SMEs and SMIs
- Group on large enterprises, focusing on raising awareness among large corporations (Commandement Opérationnel de Cyberdéfense, n.d.; Lagneau, 2013).

Once recruited, citizen reservists can join their preferred group, either in Paris or in one of the seven regional groups (Telecom SudParis, 2016).

Numbers of cyber reservists

The 2014 Cyber Defense Pact stated the necessity to create a cyber reserve. The plan was to develop a cyber reserve reaching 4,440 reservists (40 permanent personnel, 400 operational reservists, 4,000 operational citizen reservists) and 150 citizen reservists by 2019 (Délégation à l'information et à la communication de la défense, 2016; Gouvernement.fr, n.d.; Ministère de la Défense, 2016, 2014). However, the decision of June 2018 to abandon the operational citizen reserve, which was supposed to consist of 4,000 reservists, has rendered this structure obsolete. In 2019, the cyber reserve counted 200 operational reservists, but COMCYBER recognized that it needed 400 operational reservists to be fully operational. It intends to reach this number in the coming years (Lesellier de Chezelles, 2019).

The CRPOC was created with the purpose of centralizing the recruitment of cyber reservists (top-down), but in practice recruitment can also occur at the level of the unit that wishes to employ a particular reservist (bottom-up) (COMCYBER official 1, 2019). However, COMCYBER would like all recruitments to be centralized to optimally map available capabilities in the reserve and ensure the efficient allocation of resources (COMCYBER official 2, 2019).

Organization of the service: Length of military service and refresher trainings

Once recruited, operational reservists become members of the armed forces by signing a renewable three-year contract called "commitment to serve in the reserves". In this contract, they agree to serve part-time (from five to 30 days annually) in the military. They can be ordered to serve up to a maximum of 120 days in a year (*Code de la Défense – Article L4221-4,* 2018). The operational reserve is placed under the command of COMCYBER (Ministère de la Défense, 2016).

Citizen reservists do not need to sign a contract, but they receive accreditation for their status as public servants. However, given that they are unpaid volunteers, they are under no obligation to serve and can choose when they want to serve (Ministère de la Défense, 2016).

15 This company is an Army unit under the command of COMCYBER; it specializes in operational cyberdefense during deployments abroad.

Links between the armed forces and the private sector regarding the reserve

To make the reserve more attractive to citizens, employers and universities, the Ministry of the Armed Forces established a partnership called the Reserve-Corporation-Defense Partnership. In this partnership, employers and universities commit to supporting their employees' and students' service in the reserve by supporting them under a specific human resource policy. This policy aims at protecting employees and students during their service and bringing the private sector closer to the armed forces. In return, employers and universities get tax cuts, access to training programs by the Ministry of the Armed Forces and access to the network of firms involved in the partnership (Ministère des Armées, 2017). In 2017, 400 enterprises and universities had already joined the partnership (Ministère de l'Intérieur and Ministère des Armées, 2017).

Post-reserve duty (career and keeping ties with the armed forces)

Currently, no operational reservist has completed the term of their contract. Therefore, it was not possible to evaluate whether they keep in touch with the French armed forces and/or their units or whether these reservists will renew their contracts. Most of them already work in cybersecurity, and it is therefore likely that the majority of them will continue to work in the field after their reservist contract ends.

Furthermore, there is currently no club or association of current or former cyber reservists (COMCYBER official 2, 2019).

Roles	Coordinator	Expert	Analyst	Technician
Type of reserve	Permanent personnel or operational reservists	Operational reservists	Operational reservists	Operational reservists
Civilian profile	Managers	Senior cybersecurity professionals	Technicians through to engineers	Students or recent graduates
Skills required	– Leadership – Project management – Liaison with other services	– Advanced knowledge of typical systems and platforms (e.g. Active Directory) – Skills on specific systems (e.g. SCADA)	– Ability to qualify as first responder for incidents – Ability to provide relevant information to the hierarchy	– Basic technical skills
Responsibilities	Manage teams of reservists	General and specific expertise	Network surveillance and incident investigation	Simple technical tasks

Table 2: List of roles and responsibilities in the cyber operational reserves (Ministère de la Défense, 2016)

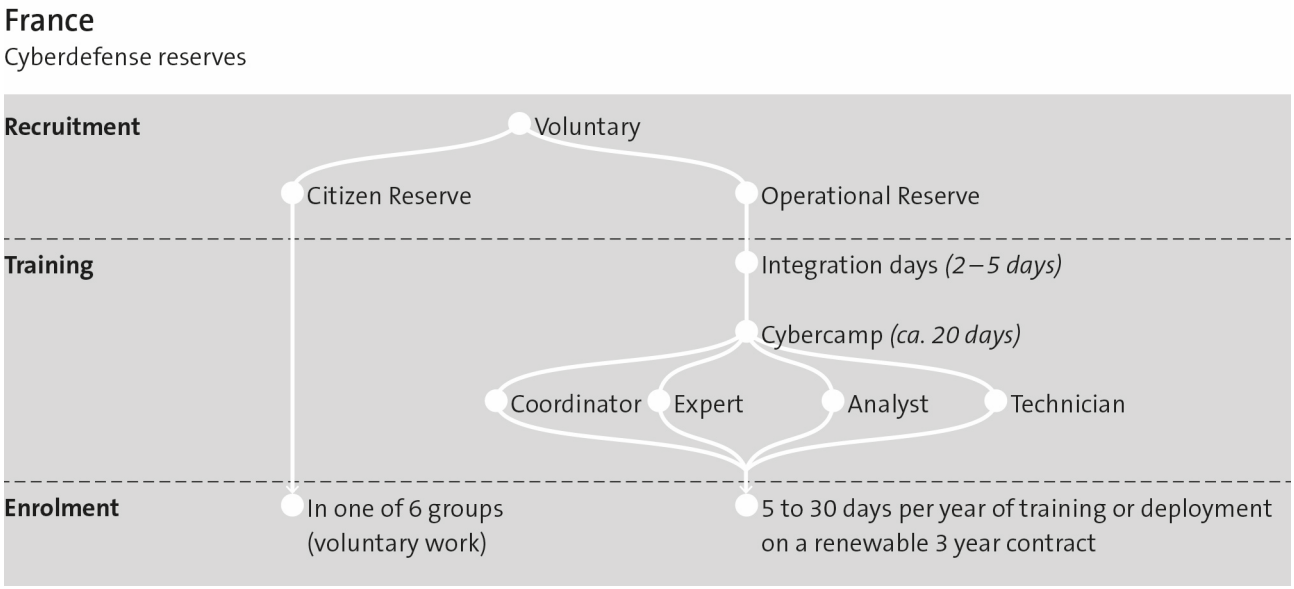

Figure 3: Journeys of French citizen and operational cyber reservists

3.4 Israel

Israel is a unitary parliamentary republic with a tradition of a conscription-based military. Since its creation in 1948, the state of Israel has been involved in several conflicts with its neighbors, and the high level of tensions between Israel and its neighbors drive the country to maintain a conscription-based military. Israel is a close ally of the US and is suspected of possessing nuclear capabilities. Israel is neither a member of NATO nor of the EU.

The Israel Defense Forces (IDF) is primarily composed of conscripts, with almost 170,000 active-duty personnel (permanent employees and conscripts) and 465,000 reservists[16] (International Institute for Strategic Studies, 2018).

Cybersecurity has been a major preoccupation of the Israeli state and IDF for a long time. Israel's Unit 8200, i.e. the signal intelligence and cybersecurity unit of the IDF, emerged after the Arab-Israeli war of 1973, as the Israeli authorities wanted to address a number of shortcomings in the country's intelligence organizations. Unit 8200 was created by merging several intelligence units and has changed its name repeatedly over time to finally become Unit 8200, the largest unit within the IDF (Kidon, 2008; Reed, 2015). The Unit's members realized during the 1990s that cybersecurity would afford opportunities for the intelligence field, and they integrated this aspect in the Unit's tasks and means (Rapaport, 2019). Therefore, the Unit specializes in signal intelligence, cyber operations and technological research and development (Behar, 2016). The Unit is surrounded by tight secrecy, making relevant information scarce.

Recruitment process and training

All Israeli citizens (male and female) who are not Arab are conscripted for military service. The IDF calls conscripts for their recruitment process, which includes a full day of medical examinations and interviews. Depending on the results, conscripts are then called to enlist for basic military training (Israel Defense Forces, 2015).

Unit 8200 runs a screening process through public and private programs for high school students in order to recruit young talents (Reed, 2015). Unit 8200 prefers young talents without university degrees to be able to educate them specifically for their tasks within the Unit (Rapaport, 2019). Further admission tests consist of psychological, socio-metric, education, and skills tests and rigorous interviews by current Unit members (peers rather than high-ranking officers). Prospective Unit members are primarily tested on mathematic, computer and language skills and more specifically on their ability to learn fast.[17] The screening process can sometimes take more than six months (Behar, 2016; Tsipori, 2017). As the Unit's reputation grows within Israeli society, the selection process is becoming more competitive (Tsipori, 2017).

Once accepted to Unit 8200, conscripts go through six months of training specific to their tasks within the Unit, unless they lack prior military training, in which case they initially go through short, basic military training, usually for three weeks (Rapaport, 2019). The training at Unit 8200 is based on practice and simulations as far as possible. Conscripts learn to produce intelligence, leverage signal intelligence and use various data mining techniques, but also receive leadership training (Sanchez, 2019; Tendler, 2015).

Conscripts who complete their military service in Unit 8200 do not receive any certification for the skills and/or knowledge they acquire. However, the Unit's reputation constitutes sufficient evidence of former members' abilities (Bar and Schechter, 2015; Reed, 2015).

Roles, tasks and responsibilities of reservists enrolled in cyber reserve

Soldiers recruited to Unit 8200 work in small teams, each with sub-teams working on different topics. There is no vertical hierarchy among teams, which function similarly to a startup's structure. This flat structure aims to encourage communication among soldiers regardless of rank and to avoid the loss of information that may occur in regular vertical chains of command (Sanchez, 2019). Each team focuses on a specific problem and on how to solve it (Rapaport, 2019).

Numbers of cyber reservists

Forbes estimates that Unit 8200 has 5,000 members at any given time. However, this number does not differentiate between active-duty staff and reservists (Behar, 2016).

Organization of the service: Length of military service and refresher trainings

In theory, male Israeli conscripts are required to complete two years and eight months of active-duty military service, whereas female conscripts do two years. After their active-duty military service period, male conscripts join the reserve forces. The reserve forces can be mobilized in cases of emergency and for training, which consists of three weeks to a month every year until conscripts reach the age of 40 (Behar, 2016). Women serve in the reserve until they are 24 years old (refworld, 2013).

However, conscripts who join Unit 8200 tend to stay with the Unit for an average of four to five years (Be-

16 Here, the word "reservist" is defined as conscripts who have finished their active-duty military service and still need to complete refresher trainings.

17 Unit 8200 focuses on the ability to learn quickly because conscripts are available to the Unit for a minimum of approximately three years. The Unit's goal is to get the most out of these conscripts before they leave the military (Tsipori, 2017).

har, 2016). They usually complete their active-duty military time and stay on as professionals (with a contract) for another two to three years or as officers (who are required to serve longer periods of time). In terms of yearly trainings for reserve forces, the standard training format is considered to be unsuitable for cybersecurity because of the rapidly evolving nature of the field. Therefore, members of the Unit tend to stay longer within the Unit, and when they join the reserve forces, only those who pursue a civilian career in a field related to cybersecurity are called back for yearly trainings and/or emergencies (Rapaport, 2019; Sanchez, 2019).

Links between the armed forces and the private sector regarding the reserve

Unit 8200 has close ties with the private sector and makes a large contribution to the Israeli economy. Many of the Unit's former members, pushed by Unit 8200 during their military service, have started their own IT companies and maintain contact with former Unit 8200 members and the Unit itself. Forbes estimated the number of companies created by the Unit's alumni to reach approximately 1,000 (Behar, 2016). The structure of Unit 8200 allows interactions between the private sector and the Unit through Unit members. Former Unit members and reservists influence the industry through the experience they have acquired during their military service. Conversely, industry is also able to influence Unit members, who contribute their civilian experiences to the Unit. Members can also take ideas acquired during their time in Unit 8200 and develop them in the private sector. However, such ideas and developments need to be approved by the Unit to ensure that no sensitive ideas, materials or technologies are compromised (Rapaport, 2019). Unit 8200 also serves to train young individuals in cybersecurity expertise and contributes to closing the workforce gap in the private cybersecurity sector (Tsipori, 2017).

Unit 8200 also organizes networking events for its current and former members with the goal to create an Israeli Silicon Valley in Beer Sheva, where the Unit will have offices in 2020 (Reed, 2015; Sanchez, 2019).

Post-reserve duty (career and keeping ties with the armed forces)

Former members of Unit 8200 keep in touch with each other through the 8200 Alumni Association, which counts approximately 15,000 members (Reed, 2015). The group primarily organizes networking events and helps former members find work (Rapaport, 2019).

Figure 4: Possible journeys of members of Unit 8200

3.5 Switzerland

Switzerland is a federal democracy with a long tradition of conscription-based armed forces. Switzerland's armed neutrality is self-imposed and permanent and forms a central element of Swiss foreign and security policy. Swiss neutrality is active and adapted to situations (Aeschimann et al., 2004; Szvircsev Tresch et al., 2019). Therefore, Switzerland is not a member of NATO, but it is a member of NATO's PfP. Switzerland is a member of the UN but not a member of the EU. However, Switzerland maintains close relationships with the EU and is a member of the Schengen Treaty.

The Swiss armed forces are primarily composed of conscripts, resulting in a strong force with approximately 140,000 personnel (Département fédéral de la défense, de la protection de la population et des sports (DDPS), 2019).

Cybersecurity has gained in importance in the Swiss political landscape and Swiss armed forces in recent years and more especially since the RUAG incident[18] in 2016. The cyberattack on RUAG gave a political impetus for more decisive action on cybersecurity, above all in the armed forces. In the Swiss armed forces, cyberdefense is part of the Armed Forces Command Support Organisation (AFCSO) and is primarily in the hands of civilian personnel with the support of reservists. In August 2018, the Swiss armed forces launched their first cyber training program to train reservists for cyberdefense missions.[19]

Recruitment process and training

All Swiss male citizens are conscripted to military service, while female Swiss citizens can volunteer. At the age of 16 years, Swiss citizens are required to attend an information day, where conscripts are informed about the various functions available to them in the armed forces, and their recruitment days are scheduled. After their 18th birthday, they then spend two days in a recruitment center, where they undergo medical and psychological examinations, and fitness tests.[20] Conscripts are assigned their functions depending on the results of the previous tests and their civilian education. The assigned function then determines where conscripts will do their basic military training.

During the first weeks of basic military training, conscripts are informed about the cyber training program. Those interested in cyberdefense are able to express their interest and can then participate in the selection process. To be accepted to that process, recruits must:

- Be fit for military service
- Have a federal apprenticeship certificate in IT or a high school diploma or be enrolled in a university program in physics, mathematics, electrical engineering, or teaching, or be an autodidact in IT/ICT
- Be motivated to become a non-commissioned officer (NCO) (Sergeant (OR-5))
- Have a suitable personality (quick learner, stress resistant, discreet and responsible)
- Be highly motivated to follow a strenuous training course
- Pass the security clearance
- Be proficient in one national language (German, French, Italian or Romansh) and English and have a passive knowledge of a second national language (Armée suisse, 2018)

The selection process is divided into two phases. The first consists of an online test, to which participate on average 135 candidates Following the initial test, the 50 top candidates are invited for a two-day assessment (the second phase). During these two days, members of the AFCSO, career military personnel and representatives of the previous cyber training program assess candidates in terms of their social skills, personalities and more general skills. At the end of the selection process, a maximum of 20 candidates are accepted into the cyber training program (Flück, 2019).

Once accepted, recruits go through a 40-week cyber training program. The program is divided into five parts:

- Six weeks of basic military training, which is the same for all Swiss recruits independently of their future functions (this is done in parallel to the selection process)
- Seven weeks of foundational training for cyberdefense functions at the Electronic Warfare School 64
- Five weeks of specialized training
- Four weeks of NCO School
- 18 weeks of practical training. Recruits acquire the rank of sergeant (OR-5) at the beginning of this training.

The cyber training program comprises a total of 800 hours of various courses, from basic cryptology to cyber threat intelligence. At the end of the training program, sergeants can choose to take a federal exam to acquire the federal qualification of certified cybersecurity specialist, which universities of applied sciences *(Fachhochschulen)* recognize and which facilitates admission to a bachelor's degree in IT. The Department of Defence, Civil

18 The RUAG incident was the revelation to the press in 2016 that RUAG (a technology firm belonging to the Swiss Confederation) had been targeted by a cyberespionage campaign (RUAG Group, 2019, 2016).

19 Before the Swiss armed forces started its cyber training course, cyber specialists were able to voluntarily join a cybersecurity unit (Flück, 2019).

20 There is also the possibility for conscripts to complete civilian instead of military service. Legally speaking, only conscientious objectors can do civilian service. However, during the past ten years, it has been easier for conscripts to choose to do civilian instead of military service. Civilian service takes the form of community service but lasts one and a half times longer than military service.

Protection and Sport (DDPS) is currently discussing the possibility for universities to recognize ECTS credit equivalencies for the cyber training program.[21] In addition, the leadership training component of the program is recognized in civilian careers (Armée suisse, 2018). Following the cyber training program, cyber NCOs are currently integrated into the AFSCO's Computer Network Operations (CNO) Company. Starting in 2022, NCOs will be integrated into a Cyber Battalion, which should become fully operational in 2025. At the same time, the Swiss armed forces are developing a cyberdefense specialist staff *(Fachstab)* consisting of senior officers who have served in other military branches and have extensive civilian experience in cybersecurity (Flück, 2019).

Roles, tasks and responsibilities of reservists enrolled in cyber reserve

Swiss recruits meeting the above-mentioned requirements can choose one of three types of cybersecurity specializations:

- CNO specialist (e.g. working on software development, performing incident analyses and vulnerabilities analyses)
- Cyber Fusion Center (CFC) specialist (e.g. performing cyberthreat analyses for the DDPS and military systems, conducting technical investigations of systems, hardware and mobile devices and conducting analyses in SOC)
- Cyberdefense specialist (e.g. contributing to situation awareness in cyberspace for the armed forces; supporting, advising and training other military personnel on cybersecurity issues; and supporting intelligence on cybersecurity issues) (Armée suisse, 2018)

Recruits are distributed among these roles in keeping with the needs of the Swiss armed forces. Representatives of CNO, CFC and Cyberdefense units meet four weeks prior to practical training to discuss the distribution of recruits. Recruits' performance during the training program and their wishes are taken into account in the process (Flück, 2019).

Numbers of cyber reservists

The first cyber training program started in August 2018 with 18 recruits (Agence Télégraphique Suisse, 2018; DDPS, 2018). A second cohort of 18 recruits started the program in February 2019. In the long-term, the goal of the DDPS is to build up a cyber battalion of 400 to 600 cyber specialists (Agence Télégraphique Suisse, 2019; Flück, 2019).

Organization of the service: Length of military service and refresher trainings

Swiss cyber NCOs are required to complete 440 days of service, of which approximately 280 are basic military and leadership training, whereas officers (OF-1) are required to complete 680 days of service (Swiss Federal Council, 2017). The basic military and leadership trainings are normally done in one block, and once reservists have completed these trainings, they return to the armed forces for yearly refresher trainings of usually three weeks' duration (19 days). Swiss reservists attend military refresher trainings every year until they reach the requisite number of days. They then do not need to complete further refresher trainings but can be called in cases of emergency until 12 years after their basic military training (approximately when they turn 30 for NCOs and until the age of 40 for officers (OF-1) (Swiss Federal Assembly, 2018).

Links between the armed forces and the private sector regarding the reserve

The Swiss armed forces intend to enable recruits to complete their practical training outside the military. This idea was being tested at the time of writing this report (Flück, 2019). The plan behind this test is to have soldiers dispatched to key partners of the Swiss armed forces to receive practical training that is not limited to the military, while also supporting partners such as critical infrastructures.

Post-reserve duty (career and keeping ties with the armed forces)

At the time of writing this report, no cyber reservists had completed their full military service. However, the first cohort of the cyber training program has finished the first round of training, and there are plans to establish a private association for Swiss armed forces cyber specialists (Flück, 2019).

21 The Lucerne University of Applied Sciences and Arts already recognizes 21 ECTS credits equivalencies for the Swiss armed forces cyber training program (Flück, 2019).

Switzerland

Swiss Armed Forces

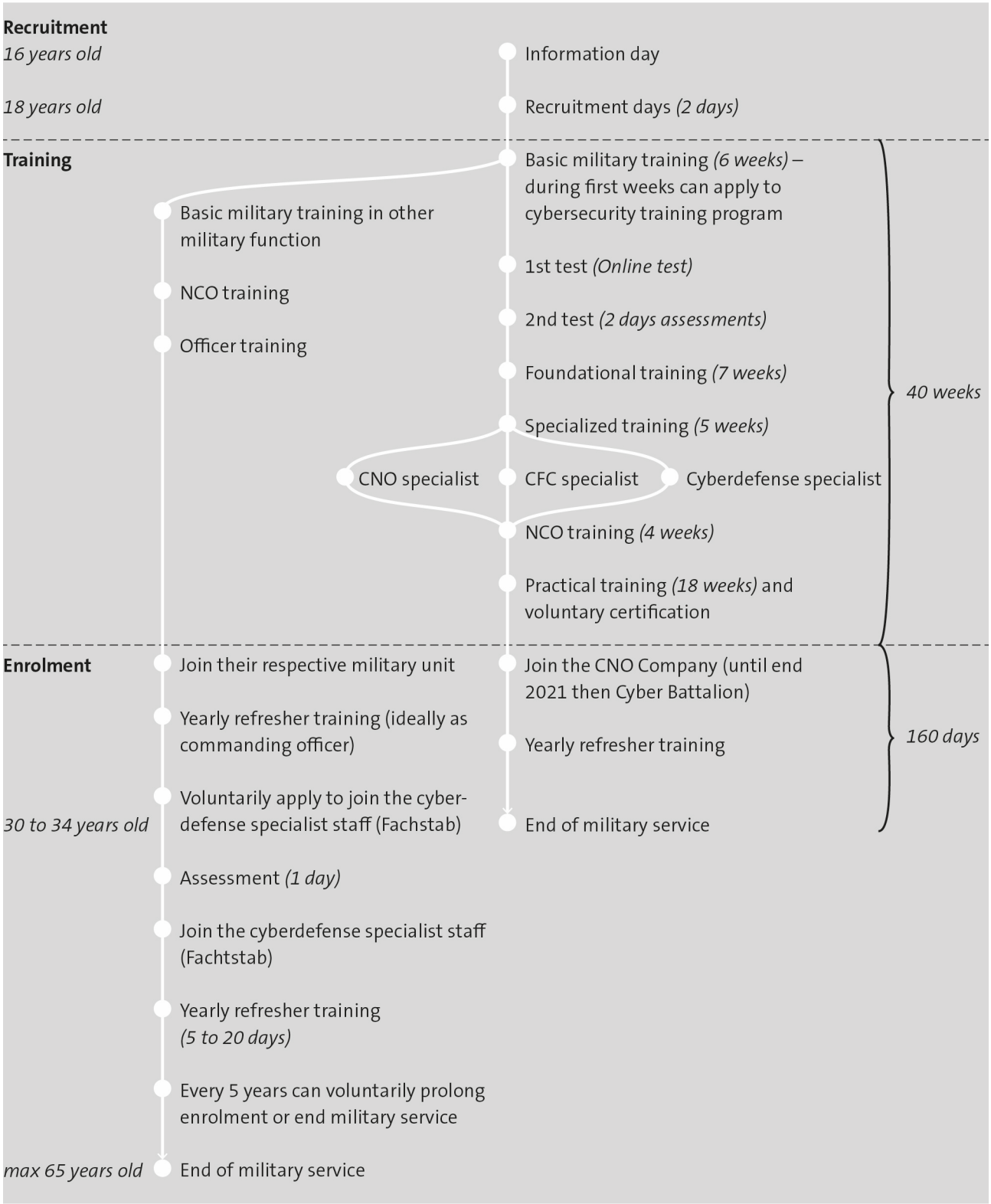

Figure 5: Possible journeys of Swiss armed forces conscripts in cybersecurity

3.6 The United States of America

The US is a federal presidential constitutional republic with large all-volunteer armed forces. The US is a permanent member of the UN Security Council, has nuclear capabilities and is considered to be a Great Power. The US armed forces are active in many theaters around the world and are involved in many active conflicts (e.g. Syria and Afghanistan). The US is a member of and main contributor to NATO.

The US armed forces are primarily composed of active-duty personnel (approximatively 1.34 million in December 2018), who are supported by reserve elements (approximatively 800,000 reserve and National Guard personnel in December 2018) (Defense Manpower Data Center, 2018). These reserve elements come from each of the military branches and can be mobilized at the federal level, while the National Guard can be mobilized at the state and federal levels (Caton et al., 2019a).

Cybersecurity has been well integrated in US policy and the US military for quite some time, with the US creating its unified cyber command, the US Cyber Command (USCYBERCOM), in 2009. USCYBERCOM, which is composed of the cyber commands of all five services (Army Cyber Command, Fleet Cyber Command/10th Fleet, Air Force Cyber/24th Air Force and Marine Corps Forces Cyberspace Command), provides a unified direction for cyber operations. USCYBERCOM also hosts all 133 Cyber Mission Force (CMF) teams. CMF forms part of the US all-force approach to cyber operations and conducts both defensive and offensive cyber operations for USCYBERCOM. All military branches are required to contribute teams to the CMF, which divides them into three groups[22] with different tasks:

- Cyber National Mission Teams, whose roles are to identify, block and defeat adversaries' activities
- Cyber Combat Mission Teams, whose roles are to support combatant commands with military cyber operations
- Cyber Protection Teams (CPTs), whose roles are to defend and protect the US Department of Defense (DoD) information network, protect missions in cyberspace, and prepare cyber forces for combat (U.S. Cyber Command Public Affairs, 2018)

Due to space and time restrictions, this study only considers organizations within the US armed forces that employ reserve elements in the CMF.[23] This is the case with the following US armed forces organizations: the US Army Reserve (USAR) and Army National Guard (ARNG) will provide 21 additional CPTs (10 US Army Reserve Cyber Operations Group (ARCOG) CPTs and 11 ARNG CPTs) to USCYBERCOM before 2024 (Porche, 2017). The US Air Force also provides five CPTs, two from the Air National Guard (ANG) and three from the Air Force Reserve (Caton et al., 2019b).

Recruitment process and training

As the US has all-volunteer armed forces, citizens need to apply for military careers (both active duty and reserve). Any individual interested in a military career first needs to contact a recruiter to go through the recruitment process. The recruitment process is the same for all branches of the US armed forces and for both active-duty and reserve. Candidates need to meet a recruiter and take knowledge, skills and medical tests. Depending on the results of these tests, individuals may be able to choose a military career in cyber operations and can then schedule the start of their basic military training (Air National Guard, 2019a; United States National Guard, 2019a).[24]

In terms of training, members of the reserve and National Guard have to go through essentially the same basic military training as active-duty personnel (10 weeks for the US Army and 8.5 weeks for the Air Force), regardless of their military occupation. Once they have completed basic military training, cyber soldiers go on to their advanced individual training for the US Army and technical training for the Air Force, where they are tested on their cybersecurity skills (Brantly, 2019). The various military branches are responsible for all four stages of training (basic individual training, individual foundation training, collective training and sustainment training) for CMF soldiers (US Government Accountability Office, 2019). As a result, cyber reservists' training may vary in terms of length and content, depending on the branch where they are employed. However, USCYBERCOM is responsible for setting standards for stages two to four to ensure minimum levels of knowledge and expertise are met. The training for reservists and the National Guard is almost the same as for active-duty personnel, with the main difference being that training is organized to be taught on weekends to suit the schedules of reservists and National Guard members. Reservists and National Guard members can also attend trainings close to where they live. Several cyber ranges and mobile training teams have been developed to facilitate access to training for reserve components (Brantly, 2019; US Government Accountabil-

22 The literature sometimes mentions a fourth group called the Cyber Support Teams. Their role is to support Cyber National Mission Teams and Cyber Combat Mission Teams.

23 Many other units in the US armed forces employ reserve elements in cybersecurity, like the ARNG that are present in Computer Network Defense Teams (CND-T) in all states and territories to protect their respective states' information networks. Annex 2 contains a table of other cybersecurity units in which USAR, ARNG, Air Force Reserve and ANG elements are engaged.

24 Active-duty personnel already active in a cybersecurity position can transfer to a reserve cyber unit. The US Army recently started to offer civilians with particular technical cybersecurity skills and a university degree the option to apply for a direct commissioning program. This program allows qualified civilians to start a military career at the rank of 1st Lieutenant (OF-1) or higher, similarly to medical doctors, legal and religious personnel (Brantly, 2019; US Army, 2019).

ity Office, 2019). The content of cybersecurity training is classified and can therefore not be described in detail in this study. However, a list of classes for the cyber operations major at the US Naval Academy and a general description of cyber training at the US Army show that cadets and cyber soldiers attend classes on technical fundamentals, programming, systems architecture, information operations, cyber operations, and planning for cyber operations (United States Naval Academy, n.d.; US Army, 2018). These classes are designed for future active-duty officers in the US Navy or the US Marine Corps and for active-duty US Army cyber specialists, but it can be extrapolated that reservists and National Guard members are required to complete similar classes to be integrated in a CPT.

Reservists and National Guard members do not receive a general certification for their positions as cybersecurity specialists in the military, but they can apply for private certifications accrediting their work on certain systems or experience (Brantly, 2019).

Roles, tasks and responsibilities of reservists enrolled in cyber reserve

Individuals opting for a cybersecurity military occupation in the reserve or National Guard can choose from a variety of jobs depending on the military branch. Table 3 depicts and describes these military occupations.

ARNG and USAR CPTs are composed of 39 members (seven officers, 16 warrant officers, 16 enlisted) organized in one headquarter element and five squads. These squads have the following responsibilities:

- Mission Protection Squad (Blue Team): responsible for protecting networks by mitigating risks, responding to incidents
- Discovery and Counter-Cyber Infiltration Squad (Hunt Team): responsible for researching and eliminating threats on friendly networks
- Cyber Threat Emulation Squad (Red Team): responsible for emulating potential threats by identifying vulnerabilities from outside networks
- Inspection Force/Cyber Readiness Squad (White Team): responsible for evaluating the CPTs' work and their operational readiness.
- Cyber Support Squad (Green Team): responsible for providing technical support to facilitate CPTs' operations and training (Caton et al., 2019a).

Air Force Reserve and ANG CPTs are organized similarly to USAR and ARNG CPTs with the exception of being referred to as Cyber Operations Squadrons and comprising 35 members. In addition, ANG has organized 12 Cyber Operations Squadrons to fill two full-time CPTs on a rotational basis (Caton et al., 2019b).

Numbers of cyber reservists

The Defense Manpower Data Center evaluated that approximately 6,300 reservists in the US armed forces were somehow involved in cyber-related military occupations in 2015 (Porche, 2017, p. 36).

At the time of writing of this report, there were no official statistics on the number of US reserve troops working in the CMF. However, it is possible to extrapolate these numbers, knowing that the USAR and ARNG will provide 21 CPTs, each with 39 members; the Air Force Reserve provides 3 CPTs with 35 members; and ANG provides 2 CPTs but with 12 rotating teams of 35 members. The estimated number of US reserve forces working in the CMF could therefore be approximatively 1,444 reservists and National Guard members[25] without counting other units in the US armed forces employing reserve elements.

Organization of the service: Length of military service and refresher trainings

Individuals who choose to join the reserve or National Guard sign a commitment for eight years, independently of the function and rank they will have in the armed forces. They can spend four to six years in drill status. Regular training consists of a weekend a month and two weeks per year. The remaining time of the commitment can be spent in individual ready reserve (for the reserve) or inactive National Guard (for the National Guard). These statuses imply that reservists would have no monthly or yearly training but could be called by the Presidential Reserve Call up Authority in cases of national emergency (Smith, 2019).

This applies to both US reservists and National Guard members involved in cybersecurity. These reservists train in their cybersecurity units for one weekend a month and complete a two-week yearly training until they transfer to the individual ready reserve or inactive National Guard.

When reserve components and/or National Guard members are activated at the federal level, they become part of the operational force. This is the case when they rotate in the CMF (Brantly, 2019).

Links between the armed forces and the private sector regarding the reserve

The USAR has a Cyber Private Public Partnership (PPP) initiative, which was launched in 2015. This initiative partners with six universities and 12 employers, including Microsoft, Verizon and T-Mobile. The main focus of this PPP is the transitioning of active-duty soldiers to the reserve and their employment and/or continuing education (Caton et al., 2019a).

25 The number that could be reached in 2024 once USAR and ARNG CPTs will be at full operational capability.

Post-reserve duty (career and keeping ties with the armed forces)

The Military Cyber Professionals Association was established in 2013 as an association for military personnel and veterans linked to the cyber profession. The goal of the association is to develop the military cyber profession and science, technology, engineering, and mathematics education in the US. The association organizes events for promoting sciences related to cybersecurity and networking; it publishes a journal and a magazine, and has a program to help former US military personnel to transition to civilian life (Military Cyber Professionals Association, 2019).

Rank/Branch	Army (USAR and ARNG)	Air Force (Air Force Reserve and ANG)
Enlisted	– Cyber Operations Specialist: conducts cyber operations – Cyber Network Defender: in charge of defensive cyber operations – Electronic Warfare Specialist: in charge of advising and assisting electronic warfare operations	– Cyberspace Warfare Operations Specialist: conducts offensive and defensive cyber operations – Client Systems Specialist: in charge of troubleshooting and repairing computers in the US Air Force – Cable and Antenna Systems Specialist: responsible for installing and maintaining cables and antennas – Cyber Surety Specialist: protects electronic systems of the US Air Force against cyberattacks – Cyber Systems Operations: maintains server and computer systems – Spectrum Operations Specialist: in charge of ensuring that nothing interferes with communication technologies – Radio Frequency Transmission Systems Specialist: in charge of deploying, maintaining and repairing communication devices – Cyber Transport Systems Specialist: deploys, maintains and repairs electronic systems – Computer Systems Programming Specialist: in charge of writing, analyzing, designing and developing applications, client-server, databases
Warrant Officer	– Cyber Operations Technician: advises officers with regard to assets and personnel for cyber operations	
Officer	– Cyber Operations Officer: plans and organizes offensive and defensive cyber operations – Cyber and Electronic Warfare Officer: in charge of conducting and coordinating electronic attacks, defense and support	– Network Operations Officer: plans and organizes cyber operations and information operations (including offensive cyber operations) – Cyber Warfare Operations Officer: plans and organizes cyber operations and information operations

Table 3: List of cybersecurity careers in the USAR, ARNG, Air Force Reserve and ANG (Air National Guard, 2019b; Caton et al., 2019b; United States National Guard, 2019b).[26]

26 This list of careers is broader than simply cyber specialists; it also includes electronic warfare showing the growing integration of cyber and electronic warfare as one domain.

USA

US Army Reserve, US Army National Guard, Air Force reserve and Air National Guard in the Cyber Mission Force

Figure 6: Possible journeys of cyber reservists in the CMF

4 Summary of findings

All six cyber reserve structures and organizations studied differ from one another. This section describes and identifies the most pronounced differences and commonalities among the six countries. These key differences are due to, among others, the fact that each country is dependent on its own bureaucracy, existing structures and strategic culture, and each cyber reserve has therefore developed within its particular context. For the most part, cyber reserves are recent, still-evolving developments.

4.1 Recruitment process and training

In the recruitment process, the most striking difference is found between conscription-based and all-volunteer armies. In conscription-based armies, recruits are required to volunteer to join the cyber training program and become cyber specialists during the first phase of their basic military training, whereas in all-volunteer armies, recruits directly volunteer for a cybersecurity position during recruitment days (depending on the results of aptitude tests).

In terms of the difference between conscription-based and all-volunteer armies, the second difference relates to cyber training programs. All armies require some sort of cybersecurity knowledge or interest prior to applicants joining the military, but the Estonian Defence League Cyber Defence Unit (CDL CDU) and French cyberdefense reserve seek to recruit volunteers with significant prior knowledge and experience. Open-source research and interviews show that the Estonian and French cyber reserves have shorter periods of initial training for their reservists because they rely on prior expertise. Their reservists, and the population that they seek to recruit, are also older compared to reservists in conscription-based armies, where recruits are commonly students with little experience. However, all countries have cyber training programs organized through the military. These programs all differ in length and focus depending on cybersecurity specialists' profiles.

Interestingly enough, not all reserves require recruits or new members to pass a test to join the cybersecurity unit. While Finland, Switzerland and Israel have very similar selection processes for their cyber reservists, requiring several rounds of tests and assessments (not necessarily focusing on cybersecurity), the EDL CDU does not require candidates to pass any test before joining the unit, and in France and the US, tests only begin once the recruitment process and basic military training have been completed.

Finally, not all cyber reserve forces deliver certifications to their recruits to authenticate the knowledge and experience of their members. Estonia and Israel do not issue certificates, arguing that being a member of their units is enough to be considered an expert in the field. Finland, in contrast, decided to issue certificates to cyber reservists. These are not specific to cybersecurity, though, as every conscript in the Finnish Defence Forces receives a certificate at the end of their service to attest to the skills and knowledge acquired or leadership training completed. In France, there is no specific certification for operational or citizen reservists, but students are able to receive university credits as equivalencies. In Switzerland, conscripts are able to take the test for cybersecurity specialist on a voluntary basis, but the armed forces do not deliver it automatically. Furthermore, conscripts who are still students should be able to validate their knowledge and skills learnt in the military by converting them into university credits in the future. In the US, cyber reservists are able to apply for certifications from providers collaborating with the US military. Therefore, cyber reservists' certifications depend on which systems they are trained on and their experience in the reserve. Not all US cyber reservists would finish their service with the same set of certifications.

4.2 Roles, tasks and responsibilities of reservists enrolled in cyber reserves

All countries examined in the case studies have their own sets of roles for cyber reservists, which vary significantly between one state and another. For some states, there are no clearly defined roles, with the focus being more on the tasks to be performed, while others have more clearly defined roles for prescribed tasks. In the US, the roles also depend on the military branch and the ranks of cyber reservists, but reservists often perform similar tasks, with their titles being the only thing that changes (cf. Table 3).

Reservists' tasks are just as varied as the aforementioned roles. However, the main commonality resides in the fact that all reservists have roles primarily focused on defense and support. These tasks consist mostly of supporting active-duty/permanent staff in protecting networks, providing education and delivering threat intelligence. Currently, only the US and Israel cyber reservists perform offensive cybersecurity tasks during their service.

4.3 Numbers of cyber reservists

Obtaining accurate statistics on the numbers of cyber reservists is complicated because of the sensitivity of the topic. However, it was still possible to estimate some of these numbers, but they remain indicative and may not reflect realities.

These estimate numbers show major disparities in the numbers of reservists, but it should be taken into account that the countries examined are very different in terms of their sizes and availability of resources. The US and Israel are obviously the ones with the largest cyber reserves, but they also have the largest armed forces and a military context that differs greatly from the others. In comparison, neutral countries such as Finland and Switzerland have much smaller units, although they are still comparable in size to France's cyber reserve.

4.4 Organization of the service: Length of military service and refresher trainings

The duration of military service varies from one case study to another. For conscription-based armies, the length of conscripts' military service differs from the length of time spent by reservists in all-volunteer armies. Conscription-based armies (except in Israel, which has a longer period of active military service) usually have recruits spend an initial one to two-year period in basic and technical military training, followed by yearly refresher trainings lasting for periods from a week to a month. In Finland, conscripts are required to complete a total of 255 to 405 refresher training days, and in Switzerland 440 to 680 days (depending on rank). In Israel, the context in which military service in general is completed differs significantly from that of the other countries studied, justifying its longer duration. In addition, some Unit 8200 members extend their military service by staying in the Unit under contract for another two to three years. In all-volunteer armies and the Estonian Defence League, members sign a contract committing to spend a certain number of days per year in military service until the end of the contract. In the US, reservists sign a commitment for eight years. but spend a total of approximately forty days per year in uniform. In France, the respective contract term is three years, but reservists spend five to 60 days per year in military service.

The way refresher trainings are organized also differs notably between one state and another. This aspect depends mostly on how military service is organized in general rather than on cybersecurity units in particular. However, in some cases cybersecurity units benefit from a separate organization. In Finland, for example, cyber refresher trainings are organized somewhat more frequently than in other military fields, as cyber technology evolves so fast. Also, in Israel, once soldiers have joined the reserve, only those who still work in cybersecurity in the civilian world continue to participate in refresher trainings.

4.5 Links between the armed forces and the private sector regarding the reserve

Reserves maintain relations with the civilian world by definition. Reservists are primarily civilians who are members of the military for a few days during the year. In all case studies examined, cyber reserves maintain some kind of relations with the private sector. In Estonia, Finland and Israel, these relations are not institutionalized and mostly informal through reservists themselves, whereas in France and the US, relations are formalized through public-private partnerships. At the time this report was written, Switzerland was testing a form of partnership, which may become formalized in the short to medium term. These partnerships are aimed at facilitating reservists' transition from the civilian to the military world and vice versa, and at promoting cooperation between the armed forces and the private sector.

All states examined maintain some sort of relations with higher education within the framework of their cyber reserves. For the majority, these partnerships serve to train cyber reservists by having university professors give courses in cyber training programs or assist in developing relevant programs and/or exercises. Higher education is also involved in developing university credit equivalencies for cyber reservists.

4.6 Post-reserve duty (career and keeping ties with armed forces)

With regard to the time after their military service, reservists do not have the same opportunities in all of the states examined. In Israel and the US, former cyber reservists are able to join alumni associations to keep in touch with former colleagues and benefit from networking events organized by these associations. In Finland and Switzerland, relevant associations are currently being developed. In Estonia, there is no official structure through which cyber reservists keep in touch with their reserve colleagues, but this is done informally. In France, there is no club or association of current or former members of the cyber reserve.

5 Challenges

The implementation of cyber reserves is part of recent development in most armed forces and is still a work in progress for most of them. While cyber reserves present some advantages, they also come with challenges. Cybersecurity is a relatively new field that needed to be addressed by existing armed forces and national security structures, and this is not an easy process. Some of the challenges pertain more generally to reserve forces rather than to cybersecurity in particular, while others are more specific to cyber reserves. Research for this study identified the following seven sets of challenges, which all six states examined in the case studies are faced with to some degree:

- How to recruit and manage the right people?
- What kind of reserve? Where to integrate it and how to coordinate with other state institutions?
- What kind of training to give to reservists?
- How to mitigate security risks associated with recruiting reservists?
- Are cyber reserves cost-efficient?
- How to manage reservists' availability?
- How to gain reservists' loyalty and commitment to the cause during and after service?

5.1 Recruiting and managing the right people

One primary reason states choose to develop a cyber reserve is to try to close the workforce gap in cybersecurity. However, recruiting reserve personnel may not be as easy as first thought and still represents a challenge for states.

Difficulties recruiting for reserves

Some states face similar challenges in recruiting both their cyber reserve workforce and their active-duty forces. In theory, it should be more appealing to candidates to join reserve forces rather than active-duty military service because it means a part-time military job with fewer constraints. However, some states struggle to find the right candidates for their cyber reserves. Finland, for example, has problems raising awareness of its cyber training program among conscripts and sometimes receives too few applications (Nokelainen, 2019). This challenge is most likely due to the fact that reservists often need to meet similar (if not the same) requirements to apply for a cyber training program as active-duty personnel (e.g. security clearance). These requirements may be a hurdle for some potential candidates for cyber reservist positions. Furthermore, salaries and the location of cyber training programs may discourage potential candidates from joining a cyber reserve. This is especially true if there is no or only a small compensation paid for the time spent in the military instead of the office, and if trainings occur in another part of the country. To counter the latter issue, and to make cyber training programs more attractive and accessible, the US armed forces have developed mobile training infrastructures to enable reservists to attend trainings in locations closer to their homes (US Government Accountability Office, 2019).

While some states are able to attract enough reservists, this does not mean that they do not face personnel challenges. Managing reservists has proven to be a serious challenge for some countries, such as France and the US. In France, the armed forces recruited several hundred operational citizen reservists, but struggled to manage them and ultimately decided to put this part of the reserve on hold and transfer it to the operational reserve. In the US, the armed forces have primarily focused on attaining operational capabilities as quickly as possible, while neglecting the readiness of CMF teams, which resulted in some teams not being certified (US Government Accountability Office, 2019). These examples illustrate cases where the armed forces recruited enough reservists but then lacked the ability to manage them to fully utilize their capabilities. They also demonstrate that a large number of reservists is no guarantee for a working cyber reserve force.

Civil service

A challenge that only concerns conscription-based armies is to attract talents who may be more interested in the civil rather than military service. This may be a significant concern for these armies, but, in practice, this challenge seems less consequential. In Finland, conscripts interested in cybersecurity would only be able to choose a cyber training program in the military service, because there is no equivalent track in the civil service (Cederberg, 2019). Furthermore, these talents may initially be lost to the FDF, but they can be recruited later, after their studies or during their career, for the hand-picked cyber reserve (Nokelainen, 2019). In Switzerland, the armed forces currently have enough conscripts applying for the cyber training program that they are able to take their pick (Flück, 2019), which compensates for the talents who choose civil service. Given that the Swiss cyber training program was only established recently, it remains to be seen whether numbers will stay stable in the future. However, conscripts opting for civil service would be demotivated if they were forced to complete military service. This lack of motivation would impact negatively on other conscripts and would be a problem for superiors in the cyber training program. These two examples show that there is a risk of losing talents to the civil service, but it tends to be overestimated. Yet this risk should not be overlooked; instead it should serve as an incentive for innovation among the armed forces in order to attract talents for military service.

Gender

Cybersecurity is often described as a male-dominated field, and this is also true among cyber reserve forces. The challenge for armed forces is to attract female volunteers. The existing gender imbalance is not specific to armed forces and also concerns the private sector. In 2019, women in cybersecurity represented 24% of the workforce ((ISC)², 2019). Therefore, armed forces are bound to miss out on talents if they fail to attract more female reservists. There is no clear difference in gender balance between all-volunteer forces and conscription-based armies. Both have a clear majority of male reservists and only a small number of female reservists. However, Israel can be considered an exception. While there are no official numbers on the members of Unit 8200, it is likely that the number of women enrolled in the Unit is proportionally higher than in the other case studies. However, this exception is likely primarily due to the mandatory conscription of both male and female citizens in Israel.

Individuals not meeting physical fitness standards for recruits

Similar to the previous challenge, armed forces risk missing out on talents by only focusing on recruiting male citizens meeting certain physical fitness standards. Cyber specialists do not need outstanding physical fitness in order to conduct cyber operations, and consequently physically impaired persons who would not qualify for regular military service would be perfectly able to work in a cyberdefense unit. Such individuals may have skills that could allow the armed forces to address shortages in their cyber workforce. However, individuals physically unfit for military service would be unable to participate in basic military training, which usually involves primarily physical activities. This could be seen as a problem, as basic military training teaches recruits fundamental military skills for defending themselves if attacked. Cyber reservists may not be on the physical frontline, but if the frontline moves toward them, they would need to be able to defend themselves. In Estonia, individuals who do not meet the required physical fitness standards for joining the Estonian Defence Forces (EDF) are still able to join the EDL CDU, as the EDL is also open to individuals unable to complete their military service (Ruiz, 2018). In Israel, the IDF recruits young people with autism for their intelligence unit, Unit 9900 (Rubin, 2016). It is likely that Unit 8200 also recruits individuals with disabilities, but no open-source information has been found to confirm this. In France, Switzerland and the US, authorities and academia are discussing the possibility of adjusting standards to allow the recruitment of physically unfit individuals (Burke, 2018; COMCYBER official 2, 2019; Reynolds, 2019; Schmuck, 2017; Schneider, 2018). While recruiting physically unfit persons may be a difficult issue to address for armed forces, as it may be interpreted as lowering physical standards, this issue should not be overlooked.

Tracking reservists' civilian careers

Reserve forces often struggle to keep track of reservists' civilian lives, causing the armed forces to potentially miss out on talents who were either not identified during the recruitment process or who were already enrolled in the military when cyber units were established. Armed forces may already have a significant pool of cybersecurity experts within their ranks without realizing. Armed forces can only become aware of such experts if they have a system for tracking their reservists' civilian careers. This is especially relevant for conscription-based armies, which have a reputation for inefficiently allocating personnel resources (Poutvaara and Wagener, 2009). In Finland, career tracking consists of a word-of-mouth-based detection system. University professors and cyber reservists are able to suggest civilian cybersecurity specialists for the hand-picked reserve (Nokelainen, 2019). In the US, members of the USAR and ARNG are asked to complete yearly questionnaires with up-to-date personal information, but this process is voluntary. Based on these questionnaires, Porche et al. (2017) estimated that approximately 10,000 members of the US Army Reserve Components have a civilian career in cybersecurity but do not work in cybersecurity in their military occupation. These two examples illustrate some ways of tracking reservists' civilian careers, but in both cases a more systematic approach would render the process more efficient. Porche et al.'s (2017) estimation demonstrates the importance of this untapped potential within reserve forces.

Changes in military career

Another challenge consists of creating processes for enabling reservists enrolled in a military function other than cybersecurity to transfer to a cyber-related military position. While reservists may have started their military careers in a military function outside of cybersecurity, they may work in this field as civilians. These reservists may be interested in transferring to cyber reserve forces, or commanding officers in cyber units may wish to have them transferred to such forces or units. Lacking or exceedingly cumbersome transfer processes result in armed forces missing out on potential talents who already meet some of the recruitment requirements. Finland uses its word-of-mouth system to identify reservists suited for transfer to the hand-picked cyber reserve (Nokelainen, 2019). In Switzerland, conscripts who have completed their military service in a different military function may voluntarily apply for transfer to the CNO Company. Similarly, commanding officers in other military positions are also able to apply for transfer to the specialist cyberdefense staff *(Fachstab)* (Flück, 2019). In France, reservists

are only able transfer to another military function after the end of their contract (COMCYBER official 2, 2019). In the US, the transfer process is long, tedious and very demanding (Brantly, 2019). These examples highlight existing discrepancies between armed forces concerning transfers from one military position to another. If armed forces wish to tap into potential expertise within their structures, they need to ensure that reservists have access to a process that enables them to move within the organization.

Maintaining the workforce

Some states may have enough reservists at present, but they also need to ensure that they will continue to do so in the future. It is one thing to have enough candidates for today's reserves, but cyber reserves currently benefit from a novelty factor and likely also from significant media coverage. However, the existing flow of candidates may decrease over time, and states need to ensure that they will have enough candidates to replace reservists ending their military service. To achieve this goal, some states have developed programs to attract teenagers to science and more specifically to cybersecurity, with Israel having the most developed programs. These programs are designed not only to attract teenagers to science, but also to identify talents for recruitment to Unit 8200. The Israeli programs involve scouting officers visiting high schools as well as two out-of-school programs, *Gvahim* (Heights) and *Magshimim* (Fulfilling), which target different demographics in Israel and train selected teenagers in programming, robotics and cyber-related fields. The Israeli government partly finances both programs (Estrin, 2017; Reed, 2015). The US has several programs, among them US CyberPatriot, CyberCorps scholarships, US Cyber Challenge and the US Cyber Academy of Excellence for Cyber Operations. These programs seek to recruit active-duty, reserve and civilian personnel. They range from scholarships for university studies in a cyber-related field to challenges and camps to encourage interest in science and cybersecurity and develop problem-solving and teamworking skills (Crumpler and Lewis, 2019; Dill, 2018). The Swiss armed forces are currently in the process of designing a program to attract teenagers' interest in cybersecurity before their 18th birthday and their recruitment to compulsory military service (Flück, 2019). Programs such as those available in Israel and the US help ensure that cyber reserve workforces can be maintained. Programs encouraging teenagers to pursue studies and/or careers in cyber-related fields benefit not only the armed forces but also the private sector, and they also help close the workforce gap.

5.2 Integration in state structures and coordination

The second set of challenges relates to the integration of cyber reserve forces into existing state security structures. Difficulties arise as new organizations or units are created and then need to be integrated into active-duty and reserve cybersecurity forces. States are also faced with the difficulty of establishing the right role for these reserve forces.

Integrating cyber reserves into existing structures

Many cyber reserve forces were only developed recently, and their development created the challenge of locating these new forces within existing armed forces structures. States had to ask themselves where cyber reservists would be positioned in relation to the armed forces, what form cyber reserves should take, who would command them, and who would supervise their work. There are no perfect answers to these questions. States need to deal with their own cultures, structures, procedures, and path dependencies to find effective ways for building cyber reserves. In all six case studies, cyber reserves were integrated into existing organizations within the armed forces rather than established as separate organizations. Cyber reserves have adopted the same or similar command structures as other reserve troops in their respective armed forces. While reservists are included in command structures, they are often supervised by permanent military and/or civilian personnel. However, the development of cyber reserve forces remains a work in progress in many states, and their infrastructure and/or organization may change with experience.

The role(s) of cyber reserves

Another challenge relates to the roles and responsibilities the armed forces should assign to cyber reserve forces. Authorities need to decide whether cyber reserve forces should focus on defensive and/or offensive operations, and whether reservists should act as support troops for active-duty personnel or perform the same duties and responsibilities as active-duty personnel. States seems to take different approaches to reservists' roles and responsibilities in times of peace or war. In general, the role of cyber reserves is primarily defensive and supportive of active-duty personnel. However, Israeli reservists also conduct offensive operations, and in the US, reservists can be activated to become part of the operational forces, which may result in them conducting offensive operations (Brantly, 2019). In peacetime, conscription-based armies focus more on defensive roles for reservists while training for possible offensive actions. Given that reservists only complete short periods of military training, armed forces most likely prefer to deploy reserve forces primarily in defensive operations, which may be more

similar to reservists' civilian jobs than offensive operations.

5.3 Skills and training

The third set of challenges concerns the skills and training of cyber reservists. Reservists are primarily civilians who attend military duty usually once a year, sometimes more frequently. The primary challenge in this context lies in the fact that the workforce is highly heterogeneous and only works part-time for the armed forces. As a result, there is only limited time available for the armed forces to shape and maintain reservists' skills.

Private sector and training

Cyber reserve forces are faced with the challenge of deciding to involve the private sector in reservists' training programs. The private sector is involved in numerous research and development projects in information and communications technologies, which may deliver technologies that the armed forces may buy and use in their daily operations. Sometimes, the private sector is the only place where reservists can be trained on a specific software or get experience in a specific environment. Therefore, armed forces need to ask themselves whether to involve the private sector in training their cyber reservists. In Finland, the private sector was initially excluded from reservist training, but the FDF ultimately decided that it should be involved (Nokelainen, 2019). The Swiss armed forces are currently testing a form of internship for cyber reservists to complete their last part of training with a private company (Flück, 2019). In the US, the USAR has public-private partnerships (PPP) with several universities and private companies (including Microsoft and Verizon), both to help reservists find jobs in the field and for continuing education (Caton et al., 2019a). Moreover, technology companies sometimes train US reservists and active-duty personnel on their products and certify them (Brantly, 2019). As the private sector is an important actor in cybersecurity, it makes sense for cyber reserve forces to collaborate with it in training and education. Relevant collaborations benefit both the armed forces, who develop closer ties with some companies and gain access to specific technologies that they may otherwise be excluded from, and the private sector, which is able to recruit new talents from among reservists.

Collaboration with higher education institutions

Similar to the previous challenge, armed forces have the choice to involve higher education institutions in their cyber training programs or not. Higher education institutions host numerous research and innovation projects in the field of technology in general and cybersecurity in particular. Armed forces are able to benefit from involving these institutions in their training of cyber forces, including reserve forces. Collaborations with higher education institutions give armed forces access to knowledge and infrastructures that they may lack. In Finland, the FDF trains its cyber specialists at the University of Jyväskylä's cyber range and collaborates with some professors in teaching conscripts (Nokelainen, 2019). Similarly, professors at Swiss higher education institutions collaborate with and teach in the cyber training program (Flück, 2019). The US armed forces have collaborated with higher education institutions for a long time, for instance through programs such as Reservist Officers' Training Corps (ROTC). Furthermore, USAR's PPP includes six universities that offer continuing education programs to reservists (Caton et al., 2019a). Armed forces should not miss the opportunity of including higher education institutions in reservist training.

Ensuring minimum skills and knowledge

With regard to reserve forces, armed forces are faced with the problem of ensuring that their reservists maintain the required skills and knowledge to ensure their operational capabilities and readiness. Reservists usually complete military service once a year, with their service primarily consisting of trainings and exercises to ensure operational capabilities and readiness in case of war or deployment. Reservists may not work in the cybersecurity field in their civilian lives or may have switched careers. As a result, their knowledge and skills may become outdated in a rapidly evolving field. In a reserve force, cyber reservists' overall knowledge is first leveled during the initial training stages. However, disparities may appear and increase among reservists once they return to their civilian lives and engage with other tasks. The necessary amount of training and maintenance of knowledge and skills depends on reservists' roles and responsibilities. Some may perform simple roles which require less training than others and for which refresher training is sufficient for skill maintenance. Others tasked with more complex duties require more training and more time to update and maintain their knowledge and skills. The latter would need more time at the beginning of refresher training before reaching operational levels again. Therefore, the period of time scheduled for refresher training needs to be flexibly adapted to ensure reservists' operational capabilities and readiness. Furthermore, armed forces should ensure that their reservists stay up to date with recent techniques and technologies while maintaining their skills in order to reduce latency times at the beginning of refresher trainings. US armed forces have faced some difficulties in maintaining the certification of CMF teams due to high turnover rates and the need to recertify teams in which more than the half of the personnel had left. Reasons for reservists deciding to leave their teams include not having completed the required

trainings, with reservists frequently falling behind in their CMF trainings because of their part-time military status. One approach USCYBERCOM employed to address this problem was to develop mobile training teams to bring trainings closer to reservists' home locations and avoid them losing time travelling (US Government Accountability Office, 2019). Among others, this example illustrates that expectations and requirements for reservists' operational capabilities and readiness were set too high when planning for reservist CMF teams, and these needed adjusting. Armed forces need to be clear about what to expect from reservists and plan trainings and refresher trainings accordingly, while taking into account that disparities in knowledge and skills may appear among reservists once they have completed the initial stages of training.

Security risks

The fourth set of challenges relates to potential security risks associated with the employment of reserve cyber forces. As reservists are not permanently employed, they may be less aware of security rules and environments than active-duty personnel and may feel these rules to be less relevant to them. Challenges regarding security risks concern the need for security clearance for reserve forces, and whether armed forces should take specific security measures to mitigate risks associated with cyber reserve forces.

Security clearance

Armed forces involving reservists in cybersecurity must decide on the level of security clearance they grant their reservists. Reservists deployed in cybersecurity, above all in military cybersecurity, will necessarily gain access to sensitive information. Armed forces require their reservists to undergo security clearance processes before they are able to join the cyber reserve. This process gives armed forces security that the reservists concerned can be trusted to work with sensitive data. Armed forces have less control over reservists than over active-duty personnel, as reservists spend the majority of their time outside the military. Therefore, armed forces must decide if they want to grant reservists the same level of security clearance as active-duty personnel. Obviously, security clearance levels need to be applied in keeping with reservists' tasks. However, security clearance processes may also deter some individuals from applying to join the cyber reserve because they may be afraid they might fail and not be granted clearance. All six countries examined for this study require their reservists to go through a security clearance process. However, France is the only country to state that it grants different levels of security clearance to reservists depending on their functions, and prevents reservists from obtaining the highest levels of security clearance (COMCYBER official 2, 2019).

Additional security measures

In addition to security clearances, armed forces can decide to take additional measures to mitigate the risk of theft of sensitive data by reservists. Security clearances indicate that a specific reservist is trustworthy at a specific moment in time, but they cannot guarantee that the same reservist may not try to steal data or disclose sensitive information in other circumstances. In many cases, reservists are also required to sign non-disclosure agreements holding them accountable if information is leaked. The French armed forces have implemented additional rules in reservists' working environments to mitigate the risk of leaks: Reservists must, for example, not be left alone and are not allowed to leave their military offices with material (COMCYBER official 2, 2019). These are examples of measures armed forces may wish to implement to mitigate risks of leaks or espionage. While each state manages its own security clearance processes, the risks of leaks or espionage by reservists should not be overlooked.

5.5 Cost efficiency

The fifth challenge concerns the cost efficiency of using cyber reservists. This challenge relates to the question of whether it is economical to invest time to train reservists, knowing that they will only be in the armed forces for a limited time and will at times be unavailable for training. Building a reserve enables armed forces to raise a considerable workforce at a lower cost than a permanent active-duty workforce. Reserve forces cost less in terms of salaries and material than permanent forces, as reservists work part-time.

However, reserves cost relatively more to train, and armed forces do not get the same return on investment as for permanent personnel. The time reservists spend in training is proportionally more significant than the time they spend applying what they have learnt in the armed forces. Furthermore, the period over which reservists implement their knowledge can become even shorter when they postpone or skip refresher trainings, resulting in additional losses for the armed forces concerned. Armed forces suffer the most severe losses when reservists quit their military service right after completing their initial trainings, well before the end of their reserve period. In order to obtain maximum benefit from reservists' capacities during their time in their military service, the Swiss armed forces and IDF try to focus their assessment and recruitment efforts on highly motivated recruits with a demonstrated ability to learn quickly (Flück, 2019; Tsipori, 2017).

Furthermore, reservist trainings tend to be strictly focused on reservists' roles and tasks for optimal efficiency. However, this form of training is narrower than a

university program, for example. Such a narrow approach may be time-efficient but can at the same time hamper reservists' ability to develop broader solutions to problems or crises.

Most cyber reserve forces are still recent, but general feedback on their capabilities is generally positive. Given their recent nature, the efficiency of most of the reserves examined in this study has not been tested in times of crisis, and it is therefore currently not possible to evaluate their performance in such times.[27] Some US states activated their US National Guard troops during the 2018 midterm elections and have announced plans to re-activate them for the 2020 presidential election (Cimpanu, 2018; The Fulcrum, 2019). The fact that states plan to re-activate these units implies that state authorities were satisfied with their work. However, the relevant teams were part of the CND-T and consequently not covered in this report. Meanwhile, the French armed forces have used cyber reservists in international deployments and stated that they were satisfied with the results (COMCYBER official 2, 2019).

5.6 Availability of cyber reservists

The sixth set of challenges relates to the organization of refresher trainings and the management of reservists and collaborations with the private sector. The primary challenge in managing any reserve forces (not only cyber reserve forces) identified in this sub-section lies in dealing with reservist availability and getting the private sector to allow employees to repeatedly leave their civilian jobs for certain lengths of time. Armed forces need to find ways to manage reservist absences such that negative impacts on unit capabilities are minimized. They also need to collaborate with the private sector and persuade it that there are benefits to having employees who are also members of a cyber reserve.

Availability of cyber reservists

A significant challenge for cyber reserve forces is managing reservists' availability. The nature of reserve forces means that reservists are only part-time military personnel whose civilian lives may at times be incompatible with military training. When reservists are able to postpone or skip military trainings, their absence constitutes a challenge for their units, which are forced to work with fewer staff. When only a few reservists postpone or skip training, it can be assumed that units still operate more or less normally without them. However, when a large number of reservists postpone or skip training, this becomes a significant difficulty for the unit. It is important for cyber reserve forces to mitigate the risk of reservist absenteeism. To do that, the states examined in this study have taken different approaches. In Estonia and in France, reservists may postpone and skip trainings. However, several reservists are trained for the same position so if one is unable to participate in training or an operation, others can take their place (Cardash et al., 2013; COMCYBER official 2, 2019). In the conscription-based Finnish and Swiss armies, reservists are obliged by law to attend refresher trainings and can only postpone refresher trainings based on strong grounds[28] (Nokelainen, 2019; Swiss Federal Council, 2017). In the US, reservists are theoretically able to postpone or skip trainings, but this is administratively difficult and impacts negatively on the advancement of their military careers (Brantly, 2019). The challenge of managing reservists' availability is important, because their absence can have a significant impact on the capabilities of a cyber unit. This challenge needs to be taken seriously, possibly as part of a broader approach rather than being merely addressed at the reservist level. Any solution will also need to include employers of reservists (i.e. the private sector).

Private-sector support

The private sector plays a significant role in reservists' lives, and armed forces need to find ways to bring the private sector to support and/or facilitate reservists' engagement. Many reservists work in the private sector, and allowing reservists to attend refresher trainings represents a financial loss for employers. As a result, employers can be disinclined to hire reservists or to release them for refresher trainings. Employers would need government incentives to compensate for their employees' absences. It can be assumed that the concept and process of refresher trainings are generally better understood and more broadly accepted across societies with conscription-based armies, including in the private sector.[29] However, even in countries with conscription-based armies, the armed forces need to communicate actively on reservists' military service and the advantages that reservists can bring to a company. A French study on the economic impact of the French National Guard found that reservists were more productive at work and were taking fewer sick leaves than regular employees. The study also found that reservist employees contribute their knowledge and skills learnt in the reserve to their civilian work

27 Unit 8200 is likely regularly involved in war-like operations, but there is no feedback or reports on its performance. Unit 8200 is also significantly different from the other five cases studied here in that IDF recruits and reservists stay longer in the military on average and in that the Unit operates in a highly specific context.

28 Swiss reservists must also pay a tax when they postpone their training. This tax is refunded once the reservist has completed military service including all military service days.

29 However, this is not always the case. In Switzerland, a firm advertised a position specifying that they would not hire candidates still completing their military service (Dejardin-Verkinger, 2017). This case shows that, as the private sector becomes more internationalized, acceptance of the tradition of conscription-based armed forces seems to be eroding.

(Goodwill-management, 2017). Investing in communicating these advantages would help the armed forces to improve reservists' employability and availability by mitigating the risks of employers refusing to hire reservists or to allow their employees to attend refresher trainings. States can also use additional measures to incentivize the private sector to employ reservists of let employees join the reserve. In France, companies employing reservists are able to join a partnership that gives them access to a network of other employers of reservists, offers them closer ties to the armed forces, and gets them tax deductions (Ministère des Armées, 2017). Such programs can help raise awareness of reserve forces, get the private sector to better understand the benefits of employing reservists, and improve collaboration with the armed forces.

5.7 Loyalty during and after service

The final set of challenges relates to the question of how to win the loyalty of reservists to encourage them to come back year after year and commit to the cause. This issue also extends to the time after military service and raises the question as to whether armed forces should keep in touch with former reservists and get involved in alumni clubs and associations.

The question of loyalty

Armed forces struggle to keep cybersecurity experts, who find better-paying jobs in the private sector. While this struggle primarily concerns active-duty personnel, reservists can also be tempted to terminate their military service early or not renew their contract if their tasks do not meet their expectations. The challenge for armed forces is to keep their reservists motivated to attend refresher trainings year after year. Given that some cyber reserves were established only recently, reservists' motivation is probably still high, but there is the risk that motivation may erode over time. Armed forces should find ways to maintain motivation. The EDL CDU tries to keep its reservists motivated by not assigning them boring tasks, involving them at the local level to be part of a community, and organizing interesting exercises (Cardash et al., 2013; Ottis, 2019). The Finnish FDF focuses on camaraderie to maintain reservists' motivation (partly by keeping teams unchanged from basic military training through to the end of military service), and conducts exercises in which reservists are able to perform operations that would be inaccessible to them in their civilian lives. Moreover, FDF cyber units enjoy a good reputation within Finnish society and are seen as some sort of special forces units. This positive reputation helps to cultivate a sense of pride among reservists, which also motivates them to participate in refresher trainings (Nokelainen, 2019). In France, COMCYBER is concerned that the motivation of operational citizen reservists may decrease after the 2018 decision to suspend this function, and that many reservists may not renew their contracts in order to transfer to the operational reserve (COMCYBER official 2, 2019). On the other hand, the French Ministry of the Armed Forces created a cyber clasp for the National Defence Medal, which is awarded to any active-duty, reservist or civilian personnel rendering particularly honorable service during military service or work (Armée de l'air, 2016). The medal highlights particular actions but also advertises the work of the Ministry's personnel and inspires others to perform similarly highly. These examples outline some measures that armed forces can implement to improve and/or maintain motivation among reservists.

Staying in touch

In addition to maintaining motivation, armed forces need to ponder whether they want to stay in contact with their former cyber reservists. Given the difficulty of recruiting cybersecurity experts, armed forces may want to stay in touch with former reservists to be able to call them back in cases of emergency even after the end of their military service. Relevant efforts would provide armed forces with access to an additional *ad hoc* pool of experts that they already know and trust. While this may be an advantage for armed forces, former reservists would also need to obtain some benefits from the process. Some alumni clubs and associations of cyber units exist in some countries, but the armed forces are generally not involved. These clubs and associations constitute suitable points of contact for the armed forces to keep in touch with former reservists. Another way for armed forces to stay in touch would be to form pools of volunteer experts from among former reservists, similarly to the Swiss Humanitarian Aid Unit. This unit allows humanitarian aid experts to join a pool of volunteer experts and be deployed as needed for specific humanitarian missions all over the world (Département fédéral des affaires étrangères, 2018). Similarly, former reservists could voluntarily join a pool of cyber experts to support the armed forces in times of emergency or for specific tasks for which the armed forces may lack relevant knowledge.

6 Conclusion

This report examined six cyber reserve forces in terms of their organization, structure and challenges faced in order to answer the following three questions:

- What are the different types of cyber reserves? How are they structured? How are they organized?
- What are the advantages of having cyber reserves?
- What are the challenges faced by states when setting up or having a cyber reserve force? How to face these challenges?

The report answers all of these questions. Regarding the nature, structure and organization of cyber reserves, the report finds that the development of reservist forces strongly depends on the respective country's context. Therefore, the broad range of countries examined identifies a variety of cyber reserve structures and organizations. Regarding the advantages of cyber reserves, their primary benefit resides in the fact that reserves help the armed forces to close the workforce gap in the field of cybersecurity. Finally, in terms of challenges faced by states with cyber reserves, the report shows that cyber reserves are works in progress. The report's final sub-section looks into possible further research on cyber reserve forces.

6.1 The importance of context

The observations and comparisons of all six case studies bring to light that the organization and structure of cyber reserve forces strongly depend on the context of the respective state. A comparison of the six states examined reveals substantial differences in structure and organization, which highlight that there is no "one-size-fits-all" type of cyber reserve force. The idea of taking one country's reserve model and transferring it to another simply does not work and is essentially bound to fail. This is because cyber reserves are dependent on their respective state's strategic culture, political institutions, armed forces structure, resources and political context. These elements ensure that each cyber reserve force is unique and tailored to fit its country's context.

However, the uniqueness and custom structures of reserve forces do not mean that states cannot be inspired by other countries' cyber reserve forces. For example, it appears that the second assessment in the recruitment process for the Swiss armed forces' cyber training program is inspired by the recruitment process of the Israeli Unit 8200. In the Swiss assessment, candidates are not only tested on their technical skills, but also on their teamworking abilities and general knowledge. Moreover, examiners include technical professionals and current members of the program (Flück, 2019). This process resembles Israel's recruitment process, in which candidates are tested on a variety of subjects and are interviewed by current Unit members (Behar, 2016; Tsipori, 2017). It is likely that other reserves have also chosen to copy or adapt elements of other reserves.

It is worth mentioning that Israel's Unit 8200 is often considered to be the perfect example of a functioning cyber reserve. The Unit recruits the best candidates, and many of its alumni build successful startups. However, Unit 8200 was developed in a very particular context that cannot be replicated anywhere else. Therefore, copying Israel's cyber reserve model in another country would not work. States should rather focus on developing their own model of cyber reserve forces to ensure that it fits their individual national goals and institutional structures. However, nothing prevents states from drawing inspiration from certain elements of other states' cyber reserves and adapting some of these ideas to their own contexts.

6.2 Closing the gap

As mentioned in the introduction, reserve forces can be considered as an option for armed forces to try to close the workforce gap in cybersecurity. This report has shown that, when armed forces manage their reserve forces properly, reserves indeed help to close this workforce gap by having non-permanent personnel perform relevant tasks. All armed forces have difficulties hiring permanent personnel, but reserve positions seem to be valued more highly and filled more easily. Armed forces will need to continue to communicate about and advertise their reserve forces in order to maintain the flow of candidates applying for cyber reserves. While the novelty of the field plays a role in boosting demand for cybersecurity specialists, it is likely that the labor market in the field of cybersecurity will balance out, as is argued by Libicki et al. (2014). Indeed, both states and private actors have invested significant resources into promoting education and training in cybersecurity-related fields. Given that these initiatives will bring new workers onto the labor market in the medium to long term, the market will return to a new equilibrium. This development will likely impact on the flow of candidates applying to join cyber reserve forces with either a flattening of or an increase in the number of candidates.

6.3 A work in progress

An examination of the challenges faced by cyber reserve forces reveals that these forces generally continue to be works in progress. The development of cyber reserves only started during the past ten years in the earliest cases, and even more recently for others. States are still

testing the development of cyber reserve forces through trial and error. With its suspension of recruitment and subsequent abandonment of the citizen operational reserve, France is an excellent example of this process. Difficulties in the management of citizen operational reservists caused the French armed forces to abandon this form of cyber reserve and transfer reservists to the operational reserve (COMCYBER official 2, 2019). During interviews conducted for this report, several interviewees stressed the fact that cyber reserve forces are works in progress and that their current form may change in the future. This indicates that states seem to be learning from their mistakes and adapting their cyber reserve forces accordingly to better fit their strategic goals and resource limitations. This experimental stage is likely to continue for another few years until states find efficient, functional forms for their reserves.

6.4 Open questions

This report focuses on only six case studies drawn uniquely from Western countries. It therefore lacks insights into cyber reserve forces in other parts of the world like Asia, or in other geopolitical contexts. It would be interesting to conduct further research on cyber reserves in these regions. Comparisons of these reserves with a focus on their organization and challenges could help to identify other possible approaches to the development of cyber reserve forces. Furthermore, given that this report concluded that cyber reserves are works in progress, it would be interesting to conduct another study on the same six countries in five years' time. The purpose of such a study would be to see how these cyber reserves have evolved, and whether their structure or organization has changed. Finally, a study comparing states with cyber reserves with states without cyber reserves would be interesting in order to uncover any significant differences. Such a study would provide insights into commonalities and differences between relevant states.

7 Annex 1

Table 2: Comparative table of the six case studies.

	Estonia	Finland	France	Israel	Switzerland	USA
Type of government	Unitary parliamentary republic	Unitary parliamentary republic	Unitary semi-presidential republic	Unitary parliamentary republic	Federal semi-direct democracy under a multi-party parliamentary directorial republic	Federal presidential constitutional republic
neutral	no	yes	no	no	yes	no
Member of NATO	yes	no	yes	no	no	yes
Member of the EU	yes	yes	yes	no	no	no
size armed forces in 2017[1]	6,600 active duty, 12,000 reserve, 15,800 paramilitary	21,500 active duty, 227,500 reserve, 2,700 paramilitary	203,000 active duty, 72,000 reserve, 103,000 paramilitary	175,000 active duty, 465,000 reserve, 8,000 paramilitary	140,000 active duty and reserve personnel[2]	1.35 million active duty, 858,000 reserve
Recruitment process and training						
Volunteers vs conscripts	All volunteers	Conscripts but need to apply within the military service to join cybersecurity training	All volunteers	Conscripts but have to go through pre-military service training (high school clubs) and still apply to join the Unit 8200	Conscripts, but need to apply within the military service to join cybersecurity training, or can apply to join the cyber general staff later if they are officers	All volunteers
Most of training in cybersecurity done before or during military service	Mostly before entering the EDL CDU but can attend training to update knowledge	Need some knowledge before military service but most of the training is provided during military service	Most of the training should be done before joining the reserve but still some training during the service	Six months of training specific to prospective tasks in Unit 8200 but need some pre-military service knowledge	Need some knowledge before military service but most of the training is provided during the military service (except for the cyber general staff)	Need some knowledge before military service but most of the training is provided during military service
Need to pass a test to get in the cyber unit?	No	Yes	No specific test for cybersecurity at the recruitment but later once start their cyber training program	Yes, but also test other skills in addition to cybersecurity knowledge	Yes, but also test other skills in addition to cybersecurity knowledge	No specific test for cybersecurity at recruitment but later once they start their cyber training program
Certification for training and/or knowledge	No	No	No but ECTS credits for reservists still studying	No but being in Unit 8200 serves as a certification	Yes but need to take it voluntarily	No specific certification but can get certification from vendors
Roles, tasks and responsibilities of reservists enrolled in cyber military work						
Roles	No defined roles	Cyber specialist	Operational reserve (coordinator, expert, analyst or technician) and citizen reserve	No defined roles	CNO specialist, Cyber Fusion Center specialist, cyberdefense specialist	Different roles depending on rank and military branch (cf. table 2)
Tasks	Support (education + support in case of emergency for private and public institutions)	Support (defending networks + programming projects + pen testing + education)	Operational reserve = support citizen reserve = awareness raising	Depends on teams but can conduct defense and/or offense operations + R&D + support	Support (software development + forensic + osint + education)	Conduct defense and/or offense operations + support

	Estonia	Finland	France	Israel	Switzerland	USA
Numbers of reservists in cybersecurity						
Numbers of reservists	No official numbers	Confidential	150 operational reservists (plan to increase to 400) and 150 citizen reservists in 2019	Estimated 5,000 members	So far 40 cyber reservists but plan to increase to 600	6,300 reservists involved in cybersecurity across the US armed forces but no official numbers for reservists in the CMF so far (estimate of approximately 1,500 by 2024)
Organization of the service: Length of reservist service and repetition courses/refresher						
Duration of military service or contract	Until the termination of the contract or expulsion	255 or 347 days of military service and 80 to 150 days of refresher trainings until 50 years old	Renewable three-year contracts for operational reservists No contracts for citizen reservists	Two years and eight months for males and two years for females of mandatory military service, but members of Unit 8200 tend to stay longer by signing a contract for two to three years	440 days for NCOs and 680 for officers (basic military training and refresher trainings) until about 30 years old for NCOs and 40 years old for officers (officers in the cyber general staff can be mobilized until they are 65 years old)	Eight years commitment contract
Annual training	Participation in activities during the year but only moral obligation to attend	Five to six days of refresher training every two to three years but can attend voluntary exercises	Five to 30 days of yearly training for operational reservists Citizen reservists choose the amount of time they invest	Only those working in cybersecurity are called for refresher trainings and emergencies	19 to 26 days of yearly refresher training	One weekend per month and two weeks of longer yearly refresher trainings
Links between the armed forces and the private sector regarding the reserve						
Collaboration with the private sector?	Not officially	Yes	Reserve-Corporation-Defense Partnership	Yes, through former members of Unit 8200	Trial with internships at private firms	PPP to facilitate the transition from active duty to reserve and civilian employment
Collaboration with higher education?	Yes for training	Yes for training	Yes, same partnership as for private sector	Likely	Yes for training	Yes for training
After reserve duty (career and keeping ties with armed forces)						
Is there a cyber reserve alumni club?	No, but members keep in touch informally	An association is in development	No	Yes, the 8200 Alumni Association (ca. 15,000 members)	An alumni association is in development	Yes, the Military Cyber Professionals Association

1 Source: (International Institute for Strategic Studies, 2018)

2 Source: (Département fédéral de la défense, de la protection de la population et des sports, 2019)

8 Annex 2

Table 3: Non-exhaustive list of other cyber-related units in USAR, ARNG, US Air Force Reserve and ANG.

Name of the unit	Component	Task(s)
Cyber Network Defense Teams (CND-T)	ARNG	Cybersecurity of the state
Virginia Data Processing Unit	ARNG	Support for cyber operations
Mobilization Day Cyber Protection Team	ARNG	Surge capacity for critical infrastructure and key missions
1st Information Operations Troop Program Unit	USAR	Support and provision of cyber and information operations expertise during training missions
335th Signal Command Det	USAR	Regional Cyber Center in Kuwait
ARCOG	USAR	Defensive cyber operations for US Army networks
ARCOG C2	USAR	Command and control for ARCOG CPTs
Army Reserve Intelligence Support to Cyber Operations	USAR	Provision of intelligence support for the offensive teams of the US Army Cyber Command
ARCC	USAR	Provision of support for the US Army Cyber Command joint force headquarters
Cyber Training Support Element	USAR	Provision of support for the opposing force during exercises
US Cyber Command Army Reserve Element	USAR	Help with planning and intelligence
Defense Information Systems Agency Army Reserve Element	USAR	Support for the DoD Information Networks mission
Defense Information Systems Agency individual mobilization augmentees	USAR	Surge capacity for Defense Information Systems Agency
US Army Cyber Command individual mobilization augmentees	USAR	Surge capacity for the US Army Cyber Command
960th Cyberspace Operations Group	Air Force Reserve	Administrative oversight over cyber reserve components
262nd Network Warfare Squadron (part of the 194th regional Support Wing) of the Washington State ANG	ANG	Cybersecurity assessments and emergency planning for the Washington State networks
299th Network Operations Security Squadron (part of the 184th Intelligence Wing) of the Kansas ANG	ANG	Real-time network security for the ANG network
177th Information Warfare Aggressor Squadron (part of 184th Intelligence Wing) of the Kansas ANG	ANG	Research of vulnerabilities and testing of US Armed Forces networks
261st Information Operations Squadron (part of the 162nd Combat Communications Group) of the California ANG	ANG	Testing of California state networks
175th Network Warfare Squadron of the Maryland ANG	ANG	Monitoring and assessment of Maryland state networks
102nd Network Warfare Squadron of the Rhodes Island ANG	ANG	Monitoring and assessment of Rhodes Island state networks
166th Network Warfare Squadron of the Delaware ANG	ANG	Support for the National Security Agency

9 Abbreviations

AFCSO	Armed Forces Command Support Organisation – Switzerland
ANG	US Air National Guard
ANSSI	National Cybersecurity Agency of France
ARCOG	US Army Reserve Cyber Operations Group
ARNG	US Army National Guard
CFC	Cyber Fusion Center - Switzerland
CMF	Cyber Mission Force - USA
CND-T	Computer Network Defense Team - USA
CNO	Computer Network Operations
COMCYBER	French Cyber Command
CPT	Cyber Protection Team - USA
CRPOC	Centre de Réserve et de Préparation Opérationnelle de Cyberdéfense - France
DDPS	Swiss Federal Department of Defence, Civil Protection and Sport
DGSE	Directorate-General for External Security - France
DoD	US Department of Defense
ECTS	European Credit Transfer System
EDF	Estonian Defence Forces
EDL	Estonian Defence League
EDL CDU	Estonian Defence League Cyber Defence Unit
EU	European Union
FDF	Finnish Defence Forces
IDF	Israel Defense Forces
NATO	North Atlantic Treaty Organization
NPF	Non-Proliferation Treaty
PfP	NATO's Partnership for Peace
PPP	Public-Private Partnership
SISA	Estonian State Information System's Authority
SME	Small and Medium-Sized Enterprises
SMI	Small and Medium-Sized Industries
SOC	Security Operation Center
UN	United Nations
USAR	US Army Reserve
USCYBERCOM	US Cyber Command

10 Bibliography

Aeschimann, S., Bichet, E., Catrina, C., Huser, B., Kaufmann, U., Margelist, S., Moser, H., Oswald, M., Plüss, M., Seger, P., Stüssi-Lauterburg, J., Suremann, T., Thalmann, A., Zemp, S., 2004. La Neutralité de la Suisse.

Agence Télégraphique Suisse, 2019. L'armée se défendra mieux contre les attaques informatiques [WWW Document]. RTS Info. URL https://www.rts.ch/info/suisse/10180221-l-armee-se-defendra-mieux-contre-les-attaques-informatiques-.html (accessed 4.16.19).

Agence Télégraphique Suisse, 2018. L'armée a lancé le premier cours de cyber-formation pour les recrues [WWW Document]. RTS Info. URL https://www.rts.ch/info/suisse/9861528-l-armee-a-lance-le-premier-cours-de-cyber-formation-pour-les-recrues.html (accessed 4.16.19).

Air National Guard, 2019a. FAQ Page [WWW Document]. Air Natl. Guard. URL https://www.goang.com/faq.html (accessed 9.4.19).

Air National Guard, 2019b. Careers - find your careers [WWW Document]. Air Natl. Guard. URL https://www.goang.com/careers/find-your-career.html (accessed 8.19.19).

Armée de l'air, 2016. La médaille de la défense nationale avec agrafe « cyber » remise à des réservistes citoyens de l'armée de l'air [WWW Document]. Ministère Armées. URL https://www.defense.gouv.fr/actualites/communaute-defense/la-medaille-de-la-defense-nationale-avec-agrafe-cyber-remise-a-des-reservistes-citoyens-de-l-armee-de-l-air (accessed 10.25.19).

Armée suisse, 2018. Instruction en cybernétique.

Bar, M., Schechter, R., 2015. Beyond Israeli Army Unit 8200 – that's not what Startup Nation is all about [WWW Document]. Geektime. URL http://www.geektime.com/2015/05/31/beyond-israeli-army-unit-8200-thats-not-what-startup-nation-is-all-about/ (accessed 10.5.19).

Bauer, T.K., Bender, S., Paloyo, A.R., Schmidt, C.M., 2012. Evaluating the labor-market effects of compulsory military service. Eur. Econ. Rev. 56, 814–829. https://doi.org/10.1016/j.euroecorev.2012.02.002

Behar, R., 2016. Inside Israel's Secret Startup Machine [WWW Document]. Forbes. URL https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/#599258bb1a51 (accessed 1.3.19).

Brantly, A., 2019. Interview with Dr. Aaron Brantly.

Burke, C., 2018. The Pentagon Should Adjust Standards for Cyber Soldiers — As It Has Always Done [WWW Document]. War Rocks. URL https://warontherocks.com/2018/01/pentagon-adjust-standards-cyber-soldiers-always-done/ (accessed 10.24.19).

Cardash, S.L., Cilluffo, F.J., Ottis, R., 2013. Estonia's Cyber Defence League: A Model for the United States? Stud. Confl. Terror. 36, 777–787. https://doi.org/10.1080/1057610X.2013.813273

Caton, J.L., Army War College (U.S.), Strategic Studies Institute, 2019a. Examining the roles of Army Reserve component forces in military cyberspace operations.

Caton, J.L., Army War College (U.S.), Strategic Studies Institute, 2019b. Implications of Service Cyberspace Component Commands for Army Cyberspace Operations. Strategic Studies Institute and U.S. Army War College Press, Carlisle, PA.

Cederberg, A., 2019. Interview with Aapo Cederberg.

Cimpanu, C., 2018. States activate National Guard cyber units for US midterm elections [WWW Document]. ZDNet. URL https://www.zdnet.com/article/states-activate-national-guard-cyber-units-for-us-midterm-elections/ (accessed 10.25.19).

Code de la défense - Article L2171-1, 2011. , 2011-892.

Code de la Défense - Article L4221-4, 2018. , Code de la défense.

COMCYBER official 1, 2019. Interview with a COMCYBER official.

COMCYBER official 2, 2019. Interview with a COMCYBER official.

Commandement Opérationnel de Cyberdéfense, n.d. La réserve citoyenne cyberdéfense en 11 questions.

Crumpler, W., Lewis, J.A., 2019. The Cybersecurity Workforce Gap. Center for Strategic & International Studies.

Defence Forces C5 Agency, 2019. Cyber cadets train in the Locked Shields 2019 exercise [WWW Document]. Finn. Def. Forces. URL https://puolustusvoimat.fi/en/article/-/asset_publisher/kyberkadetit-kouluttautuvat-locked-shields-2019-harjoituksessa (accessed 9.5.19).

Defense Manpower Data Center, 2018. Number of Military and DoD Appropriated Fund (APF) Civilian Personnel Permanently Assigned.

Dejardin-Verkinger, A., 2017. L'entreprise qui ne voulait pas engager de militaires s'excuse [WWW Document]. Trib. Genève. URL https://www.tdg.ch/geneve/entreprise-voulait-militaires-sexcuse/story/24560291 (accessed 10.25.19).

Délégation à l'information et à la communication de la défense, 2019. Politique ministérielle de lutte informatique défensive.

Délégation à l'information et à la communication de la défense, 2018a. 2018 les Chiffres Clés de la Défense.

Délégation à l'information et à la communication de la défense, 2018b. Communiqué du ministère des Armées_ Budget 2019 : LPM année 1 [WWW Document]. Ministère Armées. URL https://www.defense.gouv.fr/actualites/communaute-defense/communique-du-ministere-des-armees_-budget-2019-lpm-annee-1 (accessed 7.5.19).

Délégation à l'information et à la communication de la défense, 2018c. La cyberdéfense [WWW Document]. Ministère Armées. URL https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/la-reserve-de-cyberdefense (accessed 2.18.19).

Délégation à l'information et à la communication de la défense, 2016. Première journée de la réserve de cyberdéfense [WWW Document]. Ministère Armées. URL https://www.defense.gouv.fr/english/actualites/articles/premiere-journee-de-la-reserve-de-cyberdefense (accessed 2.18.19).

Département fédéral de la défense, de la protection de la population et des sports, 2019. L'armée en chiffres [WWW Document]. Dép. Fédéral Déf. Prot. Popul. Sports. URL https://www.vbs.admin.ch/fr/ddps/faits-chiffres/armee.html (accessed 9.10.19).

Département fédéral de la défense, de la protection de la population et des sports, 2018. Premières expériences dans le domaine de l'instruction en cybernétique [WWW Document]. Dép. Fédéral Déf. Prot. Popul. Sports. URL https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-72271.html (accessed 4.16.19).

Département fédéral des affaires étrangères, 2018. Le Corps suisse d'aide humanitaire [WWW Document]. Dép. Fédéral Aff. Étrangères. URL https://www.eda.admin.ch/deza/fr/home/activites-projets/activites/aide-humanitaire/corps-suisse-aide-humanitaire.html (accessed 11.20.19).

Dill, K.J., 2018. Cybersecurity for the Nation: Workforce Development. Cyber Def. Rev. 3, 55–63.

Durand, C., 2019. FIC : à la recherche de 1000 cybercombattants, l'armée veut faire rêver les geeks [WWW Document]. Cyberguerre. URL https://cyberguerre.numerama.com/807-fic-a-la-recherche-de-1000-cybercombattants-larmee-veut-faire-rever-les-geeks.html (accessed 6.20.19).

Estonian Defence League, 2019a. Estonian Defence League's Cyber Unit [WWW Document]. Est. Def. Leag. URL http://www.kaitseliit.ee/en/cyber-unit (accessed 2.19.19).

Estonian Defence League, 2019b. Frequently Asked Questions [WWW Document]. Est. Def. Leag. URL http://www.kaitseliit.ee/en/frequently-asked-questions (accessed 2.19.19).

Estrin, D., 2017. In Israel, teaching kids cyber skills is a national mission [WWW Document]. APnews. URL https://apnews.com/e477309a4a1e407ca4ae6568d3035625

Flück, R., 2019. Interview with Colonel Robert Flück.

Goodwill-management, 2017. Performance Economique du Réserviste l'entreprise, le réserviste et la Nation. Goodwill-management, Paris, France.

Gouvernement.fr, n.d. Les réserves de cyberdéfense [WWW Document]. Gouvernement.fr. URL https://www.gouvernement.fr/risques/les-reserves-de-cyberdefense (accessed 7.5.19).

International Institute for Strategic Studies, 2018. The military balance 2018.

(ISC)^2, 2019. Women in Cybersecurity: Young, Educated and Ready to Take Charge, (ISC)^2 Cybersecurity Workforce Study. (ISC)^2.

(ISC)^2, 2018. Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens, (ISC)^2 Cybersecurity Workforce Study. (ISC)^2.

Israel Defense Forces, 2015. The Path to Becoming an IDF Soldier [WWW Document]. Isr. Def. Forces. URL https://www.idf.il/en/minisites/soldiers-of-the-idf/the-path-to-becoming-an-idf-soldier/ (accessed 10.7.19).

Kaska, K., Osula, A.-M., Stinissen, J., 2013. The Cyber Defence Unit of the Estonian Defence League Legal, Policy and Organisational Analysis.

Kidon, A., 2008. Unit 8200: In the Beginning [WWW Document]. Isr. Def. Forces. URL https://web.archive.org/web/20090206103120/http:/dover.idf.il/IDF/English/News/today/2008n/09/0101.htm

Lagneau, L., 2013. Le réseau de la Réserve Citoyenne Cyberdéfense dévoilé [WWW Document]. Zone Mil. Opex 360. URL http://www.opex360.com/2013/04/03/le-reseau-de-la-reserve-citoyenne-cyberdefense-devoile/ (accessed 10.7.19).

Lesellier de Chezelles, B., 2019. Interview with French COMCYBER Chief of Staff Bertrand Lesellier de Chezelles.

Libicki, M.C., Senty, D., Pollak, J., 2014. H4cker5 wanted: an examination of the cybersecurity labor market. RAND, Santa Monica, Calif.

Lomsky-Feder, E., Gazit, N., Ben-Ari, E., 2008. Reserve Soldiers as Transmigrants: Moving between the Civilian and Military Worlds. Armed Forces Soc. 34, 593–614. https://doi.org/10.1177/0095327X07312090

Military Cyber Professionals Association, 2019. Military Cyber Professionals Association [WWW Document]. Mil. Cyber Prof. Assoc. URL http://public.milcyber.org/about/mission (accessed 8.19.19).

Ministère de la Défense, 2016. La réserve de cyber-défense Guide explicatif.

Ministère de la Défense, 2014. Pacte Défense Cyber 50 mesures pour changer d'échelle.

Ministère de l'Intérieur, Ministère de la Défense, 2016. Parce que la défense et la sécurité nationales sont l'affaire de tous !

Ministère de l'Intérieur, Ministère des Armées, 2017. Le Réserviste en entreprise, une action de Responsabilité Sociétaleà valoriser!

Ministère des Armées, 2017. Partenariat réserve-entreprise-défense [WWW Document]. Ministère Armées. URL https://www.defense.gouv.fr/reserve/reserve-et-entreprises/partenariat-reserve-entreprise-defense/partenariat-reserve-entreprise-defense (accessed 8.5.19).

Ministry of Defence, 2019. Share of Defence spending of total state expenditure [WWW Document]. Minist. Def. URL https://www.defmin.fi/en/tasks_and_activities/resources_of_the_defence_administration/finances/share_of_defence_spending_of_total_state_expenditure (accessed 9.5.19).

Ministry of Interior, 2019. Civilian Intelligence Act to improve Finland's national security [WWW Document]. Minist. Inter. URL https://intermin.fi/en/article/-/asset_publisher/siviilitiedustelulaki-parantaa-suomen-kansallista-turvallisuutta (accessed 9.5.19).

Nokelainen, M.-M., 2019. Interview with Lieutenant-Colonel Mano-Mikael Nokelainen.

Ottis, R., 2019. Interview with Dr. Rain Ottis.

Porche, I., 2017. Cyber Power Potential of the Army's Reserve Component, Research report. RAND, Santa Monica, Calif.

Poutvaara, P., Wagener, A., 2009. The political economy of conscription.

Poutvaara, P., Wagener, A., 2007. Conscription: Economic costs and political allure. Econ. Peace Secur. J. 2. https://doi.org/10.15355/2.1.6

Prime Minister's Office, 2017. Government's Defence Report (No. 7/2017), Prime Minister's Office Publications. Helsinki.

Rapaport, A., 2019. Interview with Amir Rapaport.

Rauschenberg, K., 2018. Maryland National Guard trains with Estonian defense forces, celebrates 25 years of partnership [WWW Document]. Md. Natl. Guard. URL https://news.maryland.gov/ng/2018/05/16/maryland-national-guard-trains-with-estonian-defense-forces-celebrates-25-years-of-partnership/ (accessed 7.16.19).

Reed, J., 2015. Unit 8200: Israel's cyber spy agency [WWW Document]. Financ. Times. URL https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c (accessed 3.5.19).

refworld, 2013. Israel: Military service, including age of recruitment, length of service, grounds for exemption, and availability of alternative service (March 2009-January 2013) [WWW Document]. refworld. URL https://www.refworld.org/docid/5152beb62.html (accessed 10.29.19).

Reynolds, R., 2019. The Airmen We Need: Americans With Disabilities in the Air Force [WWW Document]. War Rocks. URL https://warontherocks.com/2019/04/the-airmen-we-need-americans-with-disabilities-in-the-air-force/ (accessed 10.24.19).

RUAG Group, 2019. Facts & Figures [WWW Document]. RUAG. URL https://www.ruag.com/en/about-ruag/ruag-brief/facts-figures (accessed 10.7.19).

RUAG Group, 2016. Cyber attack on RUAG: major damage averted [WWW Document]. RUAG. URL https://www.ruag.com/en/news/cyber-attack-ruag-major-damage-averted (accessed 10.7.19).

Rubin, S., 2016. The Israeli Army Unit That Recruits Teens With Autism [WWW Document]. The Atlantic. URL https://www.theatlantic.com/health/archive/2016/01/israeli-army-autism/422850/ (accessed 10.24.19).

Ruiz, M.M., 2018. Is Estonia's Approach to Cyber Defense Feasible in the United States? [WWW Document]. War Rocks. URL https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/ (accessed 2.19.19).

Sanchez, R., 2019. Exclusive: Inside access to Israel's secretive cyber spy agency - which headhunts recruits at 16 [WWW Document]. The Telegraph. URL https://www.telegraph.co.uk/technology/2019/06/16/inside-israels-secretive-cyber-spy-agency-helping-fuel-tech/ (accessed 6.18.19).

Schmuck, P., 2017. Guy Parmelin recherche des «cyber-guerriers». Le Matin.

Schneider, J., 2018. Blue Hair in the Gray Zone [WWW Document]. War Rocks. URL https://warontherocks.com/2018/01/blue-hair-gray-zone/ (accessed 10.24.19).

Smith, S., 2019. What Is the Minimum Military Enlistment Obligation? [WWW Document]. Balance Careers. URL https://www.thebalancecareers.com/period-of-time-to-enlist-in-military-3354093 (accessed 4.4.19).

Swiss Federal Assembly, 2018. Loi fédérale sur l'armée et l'administration militaire.

Swiss Federal Council, 2017. Ordonnance sur les obligations militaires.

Szvircsev Tresch, T., Wenger, A., De Rosa, S., Ferst, T., Giovanoli, M., Moehlecke de Baseggio, E., Reiss, T., Rinaldo, A., Schneider, O., Scurrel, J.V., 2019. Sicherheit 2019 - Aussen-, Sicherheits- und Verteidigungspolitische Meinungsbildung im Trend. Militärakademie (MILAK) an der ETH Zürich und Center for Security Studies ETH Zürich, Zürich and Birmensdorf.

Telecom SudParis, 2016. Lancement du défi Réserve Citoyenne Cyberdéfense : «Ma thèse 3.0» [WWW Document]. Telecom SudParis. URL https://www.telecom-sudparis.eu/actualite/lancement-du-defi-reserve-citoyenne-cyberdefense-ma-these-3-0/ (accessed 10.7.19).

Tendler, I., 2015. From the Israeli Army Unit 8200 to Silicon Valley [WWW Document]. Tech Crunch. URL https://techcrunch.com/2015/03/20/from-the-8200-to-silicon-valley/ (accessed 3.5.19).

The Finnish Defence Forces, 2019. Conscript 2019 A guide for you to carry out your military service.

The Finnish Defence Forces, 2017. Soldier's Guide.

The Finnish Defence Forces, 2015. Personnel Strategy of the Finnish Defence Forces.

The Finnish Defence Forces, n.d. Conscription - a Finnish choice [WWW Document]. Finn. Def. Forces. URL https://puolustusvoimat.fi/en/conscription (accessed 9.5.19a).

The Finnish Defence Forces, n.d. Kybervarusmies, Puolustusvoimien johtamisjärjestelmäkeskus [WWW Document]. Finn. Def. Forces. URL https://varusmies.fi/palvelustehtavat-ja-paikat/-/services/506 (accessed 6.20.19b).

The Finnish Defence Forces, n.d. Finnish Defence Forces C5 Agency [WWW Document]. Finn. Def. Forces. URL https://puolustusvoimat.fi/en/about-us/c5-agency (accessed 9.5.19c).

The Fulcrum, 2019. Minnesota National Guard looks to an election security deployment [WWW Document]. The Fulcrum. URL https://thefulcrum.us/minnesota-national-guard-election (accessed 10.25.19).

The Security Committee, 2016. Implementation Programme for Finland's Cyber Security Strategy for 2017–2020.

Thierry, G., 2018. Cyberdéfense: les réservistes plaident pour davantage de sensibilisation [WWW Document]. L'Essor. URL https://lessor.org/reserve/cyberdefense-les-reservistes-plaident-pour-davantage-de-sensibilisation/ (accessed 2.19.19).

Tsipori, T., 2017. 8200 graduates aren't like 23 year-olds in Texas or Norway [WWW Document]. Globes. URL https://en.globes.co.il/en/article-8200-graduates-are-not-like-23-year-olds-in-texas-or-norway-1001191294 (accessed 3.5.19).

United States National Guard, 2019a. Guard FAQs [WWW Document]. Natl. Guard. URL https://www.nationalguard.com/guard-faqs (accessed 4.4.19).

United States National Guard, 2019b. ENTER THE NEWEST DOMAIN IN WARFARE [WWW Document]. Natl. Guard. URL https://www.nationalguard.com/careers/cyber (accessed 8.19.19).

United States Naval Academy, n.d. Center for Cyber Security Studies [WWW Document]. U. S. Nav. Acad. URL https://www.usna.edu/CyberCenter/Academics/CurrentCourses.php (accessed 8.19.19).

US Army, 2019. Cyber Direct Commissionning Program [WWW Document]. US Army. URL https://www.goarmy.com/army-cyber/cyber-direct-commissioning-program.html (accessed 8.19.19).

US Army, 2018. Army Cyber Training [WWW Document]. US Army. URL https://www.goarmy.com/army-cyber/army-cyber-training.html (accessed 8.19.19).

U.S. Cyber Command Public Affairs, 2018. Cyber Mission Force achieves Full Operational Capability [WWW Document]. US Cyber Command. URL https://www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/ (accessed 4.17.19).

US Government Accountability Office, 2019. DOD TRAINING U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force (No. GAO-19-362). US Government Accountability Office.

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.