CSS CYBER DEFENSE PROJECT

NATIONAL CYBERSECURITY AND CYBERDEFENSE POLICY SNAPSHOTS

Edited by Dr. Robert S. Dewar

Zürich, September 2018

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

CSS
ETH Zurich

ETH zürich

Editor: Dr. Robert S. Dewar

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

Please cite as: Robert S. Dewar, ed. (2018): National Cybersecurity and Cyberdefense Policy Snapshots: Collection 1, 2018, Center for Security Studies (CSS), ETH Zürich.

Contents

Introduction

Robert S. Dewar
Centre for Security Studies, ETH Zürich

1. National Policy Frameworks for Cybersecurity and Cyberdefense

The goal of this publication is to understand current cybersecurity policies as a facet of a country's national security policy, and particularly how cyberdefense is embedded in a state's cybersecurity posture. In the past decade cyberconflict has been increasingly discussed at the highest political and military levels. It has also broadened as a concept to include not just cyberattacks on critical infrastructure, but acts of hybrid warfare and state-sponsored campaigns to affect or change public opinion. Cyberspace is therefore increasingly being viewed as both a strategic domain and as a tool to be used in a strategic manner. Cyberconflict itself has moved towards what Liddell Hart (1965) described as "grand strategy": all the resources of a nation state – economic, military, diplomatic, social and informational – are being deployed in both peacetime and wartime to ensure that the state and its citizens remain secure in an increasingly digital and connected world. Due to the ever-increasing availability and variety of sophisticated malicious digital tools and the ease with which these tools can be deployed, cybersecurity is now a crucial element of national security. Within this larger context, the concept of cyberdefense, with its implicit military connotation, has also gained significantly more prominence.

Defining "cybersecurity" and "cyberdefense" is problematic and presents an ongoing challenge (Kruger, 2012). National policies of the kind analyzed in the snapshots contained in this collection define these concepts very differently. However, in order to conduct an effective examination and analysis of national policy a set of base-line definitions is needed. As working definition, we understand cyberdefense to fall under the purview of a country's national security policy, and therefore is a part of its defense department or ministry, while nevertheless retaining a close a link to the overall policy efforts to improve a country's cybersecurity. As such cyberdefense intersects with cybersecurity.

Cybersecurity policies tend to be more holistic and are released into the public domain, with references to ensuring civilian that infrastructures such as banking and personal computer networks are secure and resilient to cyber intrusions, and setting out measures designed to tackle online criminal activity (cybercrime). Cyberdefense by contrast is more of a closed box. This is due to its close relationship to secret, classified aspects of government policy and activity[1]. As such, cyberdefense deserves special attention in studies of national policy such as this collection of analyses and is treated separately in the policy snapshots contained in this collection.

Since there is an overall impression that the risks to national security from cyberspace have changed both in terms of quantity (more incidents are occurring) and quality (these incidents are becoming more sophisticated), many states have re-evaluated their previous cybersecurity efforts. In the ten years to 2018 a large number of national policies and strategies have been published specifically addressing cybersecurity and cyberdefense. Although these policies and strategies address similar issues, there is significant variation in approaches given national priorities and conceptualizations of the issues at hand.

2. Purpose of the handbook: What is a "snapshot"?

This current edition explores the trends and divergences in these national policies in order to better understand how cyberdefense intersects with cybersecurity policy. In a systematic fashion we take a snapshot of the current national cybersecurity and cyberdefense policies of four important European actors – France, Finland, Germany and the United Kingdom. The collected analyses examine where these states currently stand from a policy perspective and how they deal with cyber issues.

The objective of these snapshots is to provide clear information and insight into important core aspects of cybersecurity and cyberdefense policy at the state level. This is achieved by examining current and former cybersecurity, cyberdefense and national security policy and strategy documents published by countries around the world.

The documents examined to produce these national snapshots are open-source and in the public domain. They are drawn from ministerial sources as well as publically available online repositories of such policies, including those of the European Network and Information Security Agency (ENISA)[2] and NATO's Cooperative Cyber Defense Centre of

[1] It is important to note that these definitions are intended as a baseline or starting point for analysis in order to differentiate core policy documents. They are not indented to supersede or supplant any definitions provided by the national policies under examination. National definitions, where they are provided in the policy literature, are presented in the glossaries of each snapshot.

[2] Available at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

Excellence (CCDCOE)[3]. Open-source documents were chosen for analysis to ensure that any findings or conclusions could be published and made freely available. All of the snapshots are either compiled or at least validated by national experts.

There are two consequences of basing the analysis on published policy documents that are important to note at this point. The first is that that analysis can only examine areas discussed in those documents. As a result, certain questions of interest or importance – such as the impact of new legal norms such as the Tallinn Manual or ongoing activities at European Union – can only be examined if specific mention of them is made in the policy documents. While not discussing these questions may seem like an omission on the part of the researchers and editors, they are in fact restricted by the scope of the documents used for the analysis. It is envisaged that, as the corpus of policy literature expands, so too will the areas and questions of analysis given the priorities and foci of the countries being examined.

The second consequence of basing the analysis on open-source policy documents is that that there is a concentration on de jure relationships, responsibilities and actions. De facto situations are too abstract and subjective to be included as part of an analysis and he the de facto jurisdictions of a cyber security or cyber defense agency present different questions to the ones being examined in the snapshots. An example of this can be found in the examination of the United Kingdom's Government Communications Headquarters (GCHQ). This agency is heavily involved in intelligence-gathering and works closely with the UK's Ministry of Defence. This is a de facto military relationship given the GCHQ's work. However, the GCHQ falls under the oversight of the Foreign Office and is therefore a de jure civilian entity. This civilian nature is stated in the policy literature, from which the snapshot analysis is drawn.

3. Structure of the snapshots

Each national snapshot contains four sections of analysis. Section 1 provides a timeline of document publication contextualized with major cybersecurity incidents which impacted policy development. Section 2 of each snapshot provides more detailed analysis and understanding of current policy and strategy. It zooms in on specific national security, cybersecurity and cyberdefense policy documents (where such documents exist), examines core themes, fields, tasks and priorities and extrapolates interconnections between the documents. There is a particular focus on any identifiable relationships between cyberdefense and national security policy.

Section 3 continues the focused analysis, but concentrates on the organizational structures and frameworks used to develop and implement policy. It sets out any overarching frameworks, and specifies identified relationships between the various national agencies, ministries and bureaux involved in cybersecurity and cyberdefense. The section examines any interconnections between agencies and policy documents, such as whether or not a trend exists towards centralization of leadership and policy development. An important contribution of this section is an organigram of the hierarchy and interrelationships between the national entities involved in cybersecurity and cyberdefense which provides an illustration of policy development and oversight responsibilities. The majority of the organigrams contained in this and subsequent editions have been created by the CSS using the analyses provided by the contributors. However, where such organigrams are published in the national policy documents themselves, these are used directly and sources cited. A fourth section closes each snapshot by examining any societal linkages, international partnerships and research and education programs pertinent to cybersecurity and cyberdefense.

Different countries adopt different national policy frameworks, but by focusing the snapshots on a core set of documents and examining the same broad topics for each national case study as much clarity as possible could be provided in a policy area still dogged by unclear and inconsistently applied definitions, competing priorities and a lack of conceptual standardization.

A consistently applied analytical structure and format enables international and regional trends as well as national idiosyncrasies to be identified and examined while ensuring analytical harmonization. From a practical, methodological perspective, the four-part format also serves to highlight national preferences for either considering cyberdefense as a unique policy area or as a subset of other more general strategic fields, and the operational consequences of this course of action.

In addition to the four sections outlined above, the snapshots include three graphical metrics. These are sliding scales representing the extent to which policy development and management in cyberdefense and cybersecurity is centralized; the extent to which these areas fall under civilian or military oversight and whether or not the state under examination has a defensive or offensive cyberdefense posture. A state's position on these sliding scales is derived from the policy analysis undertaken for the snapshots. If a state concentrates a significant amount of policy development and implementation responsibility in only a few or a single entity, it is reasonable to conclude that that state operates a more centralized approach to cybersecurity and defense leadership. Similarly, if the responsible entity is, or is positioned in, a defense ministry, then there will be a greater degree of military rather than civilian oversight. Finally, if the possession of offensive cyberdefense capabilities is explicitly stated in the policy literature, a state can

[3] Available at https://ccdcoe.org/cyber-security-strategy-documents.html

reasonably be said to maintain an offensive cyberdefense posture, even if specific capabilities and tools are not mentioned.

Finally, each individual snapshot contains a set of its own appendices, including a glossary of specialist terms, an explanatory list of abbreviations and acronyms and a select bibliography.

4. Future analyses

Cybersecurity and cyberdefense are constantly shifting and evolving topics. The technology used to carry out cyberattacks, and the tools required to mitigate or deter those attacks, is in a constant state of development and innovation. As a result, national policy relating to these topics also undergoes periodic shifts and changes, depending on national priorities. These policy shifts are evident in the analyses of Section 1 of each snapshot, and changes will continue to occur in the future. In order to respond to and take account of these thematic and policy developments, the snapshots contained in this edition – and those to be published in future collections – should be considered "living" documents: they will be periodically updated to demonstrate and capture any new data, events, definitions, policy developments or technological innovations of relevance. These updates will be published in successive editions of the collection, and new national analyses will be added as they are conducted.

France

Marie Baezner
Centre for Security Studies
ETH Zürich

Highlights/Summary

1. Key national trends

France is an important international and European actor. It is a member of NATO, the European Union and a permanent member of the United Nations Security Council. It also works closely on cybersecurity issues with bilateral partners such as the United Kingdom and Germany. France wants to position itself as an international power in cybersecurity. This is despite the fact that offensive cyber capabilities are rarely mentioned in cyberdefense strategies and national cybersecurity is mainly lead by the civilian entities and focused primarily on resilience.

2. Key policy principles

2.1. Cybersecurity

The French Cybersecurity Strategy has a broader perspective than purely cybersecurity issues by being named as the National Digital Security Strategy. It encompasses technical issues and cybercrime but also propaganda and "influence campaigns" led through cyberspace against France's population. The French National Cybersecurity Agency (ANSSI) is the lead agency for the civilian side of cybersecurity.

2.2. Cyberdefense

The French Cyberdefense Strategy focuses mainly on defensive measures by improving robustness and resilience. The Ministry of Defense (MoD) is the lead entity and is also responsible for the cybersecurity of its own information systems and networks.

3. Key national framework

3.1. Cybersecurity

The organizational structure of the French cybersecurity is centralized around the ANSSI. This agency is responsible for assisting the state's institutions on issues of cybersecurity, for organizing cybersecurity standards for industries and critical infrastructures, and for organizing awareness campaigns and education for civilians.

3.2. Cyberdefense

The French MoD works in parallel with the ANSSI and cooperates with its civilian counterparts through their respective analysis cells. The MoD is also responsible for the protection of its own infrastructures, for cyber offensive and defensive capabilities of the armed forces, and the development of cybersecurity products (both hardware and software).

4. Level of partnership and resources

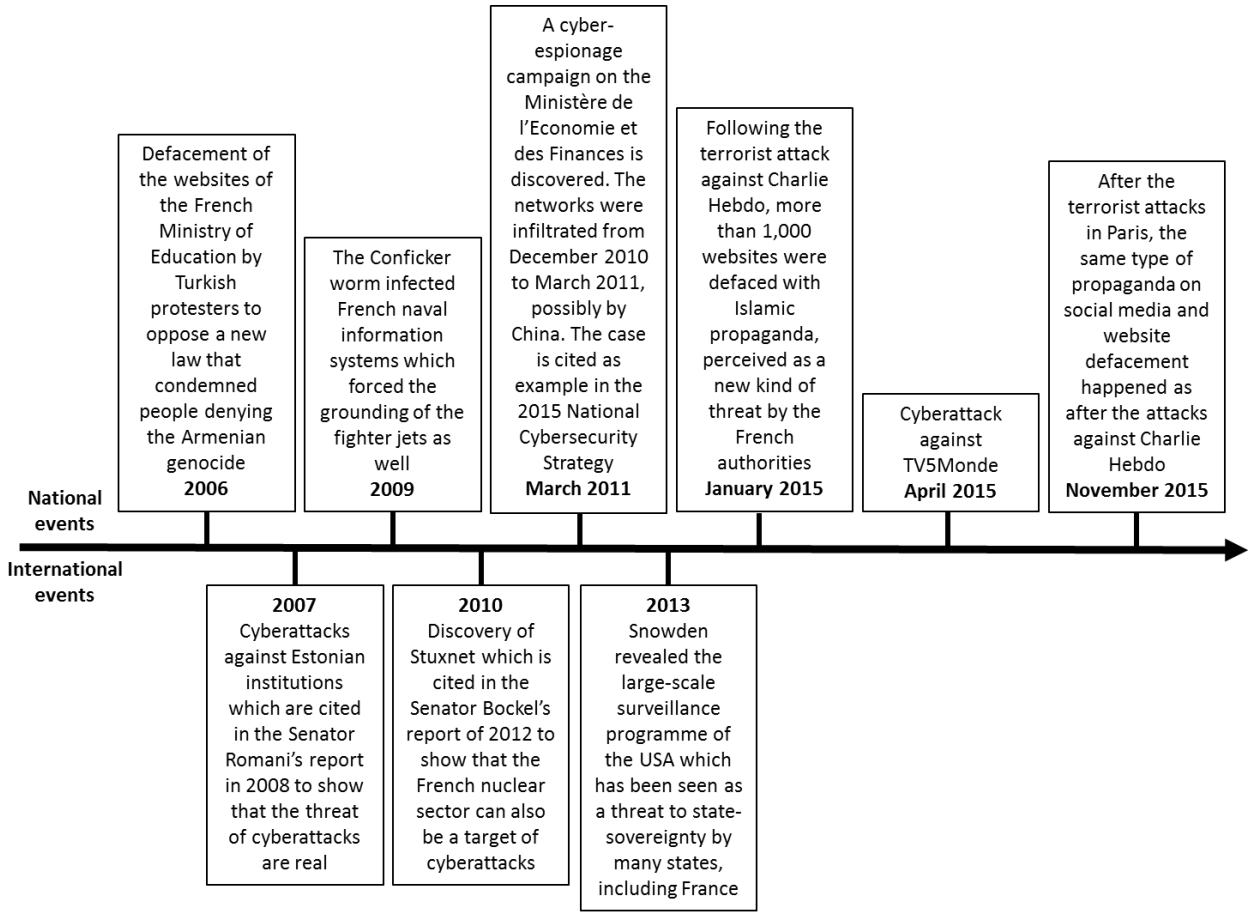
France cooperates on cybersecurity issues with its allies within NATO and the EU, but also wants to cooperate more closely with the UK and Germany on issues of cybersecurity. The strategies do not describe any public-private partnership, but the ANSSI is the main actor to set cybersecurity standards and to make sure that operators of critical infrastructures meet these standards.

1. Evolution of national cybersecurity policy (since mid-1990s)

1.1. Threat perceptions: trigger events

This sub-section describes the main domestic and international events that have had an impact on the shaping of cybersecurity and cyberdefense policies in France.

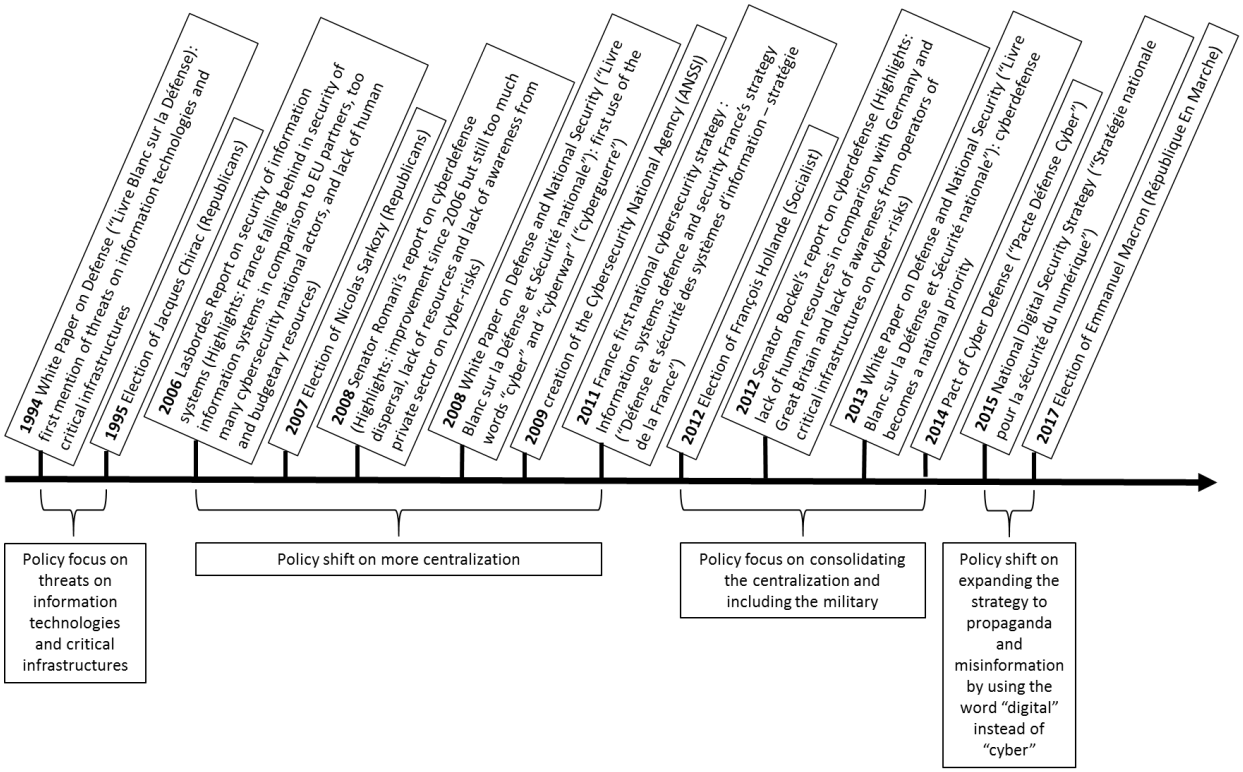
Diagram FR1: Timeline of Trigger Events



1.2. Main policy documents: key shifts in strategy

This sub-section describes the key shifts and general trends in the evolution of the cybersecurity and cyberdefense policies in France.

Diagram FR2: Timeline of Policy developments and Trends



1.3. Organizational structures: key parameters

The French organizational structure for cybersecurity and cyberdefense is highly centralized and is consistent with France's wider political structure. Leadership is centered on the National Cybersecurity Agency (ANSSI), a civilian organization supervised by the Prime Minister. While policy, including published documents, are developed by the Secretariat General for Defense and National Security (SGDNS), ANSSI focuses primarily on the social, economic, economic and governmental aspects of cyber issues. ANSSI recognizes that the French economy cannot grow without internet-related businesses and aims to promote a secure cyberspace in order to keep a competitive French economy while simultaneously ensuring users' privacy (Secrétariat Général de la Défense et de la Sécurité Nationale, 2015).

In parallel to this civilian focus from ANSSI, the French Ministry of Defense (MoD) is responsible for cyberdefense and the maintenance of its own systems and networks. The MoD cooperates with ANSSI at the level of the analysis of threats and forensics of cyberattacks (Ministère de la Défense, 2014a).

1.4. Context/Analysis: key national trends

France is a regionally and economically important nation. As one of the founding nations of the European Union (EU) and a permanent member of the United Nations (UN) Security Council, France considers itself a modern Great Power. It possesses a nuclear arsenal and does not hesitate to project power though the deployment of military forces outside its borders, in its former colonies and its areas of influence in Africa in the Middle East. As the sixth largest economy in the world and a member of the G7, France is also an important economic nation.

This projection of power is reflected in France's cybersecurity posture. The first lines of its first cybersecurity strategy of 2011 stated that France wanted to become a world power in cyberdefense (Agence Nationale de la Sécurité des Systèmes d'Informations, 2011). This statement confirms the view that France has of itself as a Great Power, a view reiterated by the former Minister of Defense Jean-Yves Le Drian, who claimed in an interview that France was one of the top cyberpowers after the USA, China and Russia (Cabirol, 2015).

Despite this view of itself France does not forget that it needs international cooperation to increase its cybersecurity. All of its strategies highlight the importance of international collaboration and the role of France in the EU and NATO.

France is an important member of NATO as it has the second largest defense budget of the European members (approximately € 40 billion for 2017 (Poncet, 2016)) and it returned to the NATO Integrated Command in 2009 (French Foreign Ministry, 2014).

In keeping with this international outlook for cybersecurity, France is an active member of other international organizations. These include the UN, the Organization for Security and Cooperation in Europe (OSCE) and the Council of Europe. France also seeks to develop closer partnership in cybersecurity with historic partners, which it calls "preferred partners", like the UK and Germany (Ministère de la Défense, 2014a).

This proactive approach can also be found in France's attitude towards military intervention, particularly in its historic areas of influence such as its former colonies. France is able and, crucially, willing to use its military forces as a foreign policy instrument as well as to protect French citizens and its national interests around the world. The fact that France's possession of cyber offensive capabilities is mentioned in both the Strategic Review on Defense and National Security and the Cyberdefense Strategy is consistent with that proactive attitude (Ministère de la Défense, 2013). As a result, on a spectrum of "civilian vs defense" posture for cybersecurity in general, France occupies a similar position to that of Germany: favoring a defense posture more than some other actors, but still retaining civilian leadership (See Annex 1).

In addition to having an active military force which it was and is willing to use, France was in a State of Emergency which lasted from its initiation in November 2015 to its official termination on 1 November 2017 (Bamat, 2017). This particular situation enabled the intelligence community and the military to have a wider scope of operation both in the cyber and physical domains, a scope they would not normally have. This State of Emergency increased pressure on a military already under pressure and overstretched due to cutbacks in the military budget.

2. Current cybersecurity policy

2.1. Overview of key policy documents

2.1.1. Strategic Review on Defense and National Security, 2017[4]

The Strategic Review on Defense and National Security published in 2017 is the new national security strategy produced by the new government of President Emmanuel Macron. The primary focus of the Strategic Review is to maintain France's strategic autonomy, a stance which relies upon the development of a high degree of technological, industrial and operational independence.

The Strategic Review is the third French national security strategy to reference cyberthreats and cybersecurity issues. It is, however, the first such strategy to utilize the changes in vocabulary initiated by the 2015 National Digital Security Strategy (see Section 2.1.2 below). In the Strategic Review, the word "digital" is used more frequently than the word "cyber", confirming that change. This indicates a decision to use a particular terminology which adds greater clarity to often vague "cyber" terminology and sets French policy apart from a number of its Western equivalents.

In the Strategic Review, digital issues and threats from the digital domain are not only described as a threat to French national security. That domain is also considered a military domain in the same manner as land, sea, air and space. This contextualization places French national security policy, as regards cyber, on a par with that of the UK and the US. The Strategic Review also clarifies that France needs to better control the industrial and legal aspects of digital technologies, hardware, software, services and data to be able to maintain its sovereignty in cyberspace. To ensure and protect this sovereignty, a number of goals are set out, including the establishment of permanent offensive and defensive cyber capabilities. These capabilities are to be reinforced along with incident detection and the attribution capabilities. It is also highlighted that networked military equipment need to be protected against cyberattacks (Ministère des Armées, 2017).

The Strategic Review, however, does not clarify the manner in which France would respond to a cyberattack. This is to be found in an earlier document, the White Paper of 2013, which stated that France would first consider diplomatic, judicial and law enforcement responses, but that the use of military means can be considered if national interests are at stake (Ministère de la Défense, 2013), reemphasizing France's ability and willingness to use its armed forces. That being the case, the Strategic Review also acknowledged that the range of possibilities of actions in cyberspace brings new opportunities for political decisions to defend national interests (Ministère des Armées, 2017).

2.1.2. National Digital Security Strategy, 2015[5]

The National Digital Security Strategy (SNSN) 2015 is the most recent strategy of the three studied in this report and details French cybersecurity policy. It is also the only document that speaks of "digital security" instead of "cybersecurity". The SNSN replaces the first cybersecurity strategy of 2011, the Information Systems Defense and Security Strategy (DSSI)[6]. The earlier document was aimed at making France a leading nation in cyberdefense by maintaining its ability to make decisions by protecting information related to the state's sovereignty, improving cybersecurity of critical infrastructures and ensuring security in cyberspace (Agence Nationale de la Sécurité des Systèmes d'Informations, 2011). In contrast, the SNSN published only four years later is a primarily civilian-oriented with very little mention of the MoD's roles in cybersecurity. Instead the focus is on the education and awareness measures described in the White Paper of 2013, but with a continued emphasis on protecting the state's sovereignty. The strategy also reaffirms the need and measures on international cooperation and education detailed in the Pact of Cyber Defense 2014 (see Section 2.1.3).

2.1.3. Pact of Cyberdefense 2014[7]

The Pact of Cyberdefense (PCD) published in 2014 is the French strategy or "plan d'action cyberdéfense". It presents 50 measures to improve the French MoD's cyberdefense. The strategy reaffirms the French cyber offensive, defensive and intelligence capabilities mentioned in the White Paper of 2013. The Pact also confirms France's intention of

[4] Revue Stratégique de Défense et de Sécurité Nationale, 2017. For consistency and ease of reading, titles of policy documents and relevant agencies will be rendered in English with English abbreviations, while original titles will be provided in footnotes. For a full list of documents, abbreviations and French-English equivalency, see Annex 3.
[5] Stratégie Nationale pour la Sécurité du Numérique, 2015
[6] Défense et sécurité des systèmes d'information – stratégie France, 2011
[7] Pacte Défense Cyber, 2014

cooperating within international organizations and alliances to improve cybersecurity, but also to enhance cybersecurity on a national basis with education and awareness campaigns.

The policy reasserts the claims of the White Paper 2013 to create and develop a Cyberdefense Reserve and a Cyberdefense Operational Reserve[8].

2.2. National Cybersecurity Strategy: fields, tasks, priorities

The National Digital Security Strategy (SNSN) is France's current cybersecurity strategy and covers a very broad range of issues. This breadth stems from an equally broad definition of cybersecurity and the use of the word "digital" instead of "cyber", even in the title of the document. A result of this ideational breadth is that the French conceptualization of cybersecurity also includes other, more societal issues such as privacy, the rights of Internet users and online propaganda. This marks a shift in French policy from earlier positions and can be interpreted as a reaction to the revelations made by Edward Snowden regarding the mass Internet surveillance conducted by the USA.

The SNSN sets out five objectives for French cybersecurity:

1. Improving cybersecurity and resilience through national and international cooperation
2. Improving French users' privacy rights and helping victims of cyberattacks and "cybermalevolence"
3. Improving education and awareness about cyber issues
4. Supporting innovation in cybersecurity
5. Lobbying EU institutions for the cyberautonomy of the EU and cyberspace stability.

As demonstrated by these five goals, the strategy is civilian-oriented and therefore positions ANSSI as the primary governmental institution addressing cybersecurity issues. Nevertheless, other important ministries are involved in this policy area. The Ministry of the Interior is responsible for law enforcement and the Ministry of Foreign Affairs manages international cooperation on cybersecurity in partnership with, and with the support of, ANSSI. Once again, this is a heavily civilian-oriented situation

Reflective of France's drive for increased sovereignty in cyberspace, also mentioned in the strategy is France's wariness of the dominance of several big Internet companies – including Amazon, Google and Facebook – on the issue of Internet users' data and the opacity with which these corporations use this data. In that regard, France has been promoting the EU's "right to be forgotten" regulation since 2009. It is clear that the use or misuse of France's citizens' data can also be perceived as an attack on state sovereignty, which also includes France's decision-making process and the use of propaganda. The latter was included in the strategy most likely as a reaction to the jihadist and pro-ISIS online messages that was published after the Charlie Hebdo attack. These online campaigns, and the physical attacks themselves, were perceived as an offense against French sovereignty by attempting to shape public opinion in favor of the jihadist cause and against French values and authorities. On these issues of privacy rights and propaganda, the SNSN makes clear that digital security is an issue that concerns the whole of society and not just state institutions (Secrétariat Général de la Défense et de la Sécurité Nationale, 2015).

2.3. National Cyberdefense Strategy: fields, tasks, priorities

The 2014 Pact of Cyberdefense (PCD) is the first document that refers directly the MoD and its institutions as being responsible for cyberdefense. That being the case, the MoD has been responsible for its own cyberdefense – i.e. ensuring the security and protection of its own systems and networks – long before the publication of the PCD.

The PCD contains six strategic goals, subdivided into specific action points:

1. Improving the robustness and resilience of the MoD's systems. The action points in this area emphasize the need to develop national cybersecurity technologies and high security standards for the MoD and its partners.
2. Preparing for the future through technical, academic and operational research. Here the action points focus primarily on providing financial support for research.
3. Increasing cyberdefense personnel, with four action points focusing on how to attract and keep cybersecurity specialists within the MoD.
4. Developing the Cyberdefense Centre of Excellence in Bretagne, with action points concentrating on the development of the Centre as a hub for cybersecurity actors.
5. Improving international cooperation with the EU, NATO and France's areas of influence. There are nine action points focused on cooperation with NATO and the EU in coordination with the Ministry of Foreign Affairs and ANSSI.

[8] The details and differences between the two reserve forces will be explained in section 3.3.1 and 4.3.

6. Stimulating the development of a national cyberdefense community with the support of the reserve.

What makes the PCD an innovative policy for France is the centralization of all cyberoperations into a single entity: the Cyber Command (COMCYBER). This is a level of centralization not previously seen in policy documents relating to this field. However, despite this new drive for centralization, the priority for French cyberdefense continues along previously established paths. The policy remains focused on improving robustness and resilience of information systems, through research, innovation and international cooperation (Ministère de la Défense, 2014a).

2.4. Context/Analysis: key policy principles

The National Digital Security Strategy of 2015 makes little mention of the MoD and the military. Whilst on the surface this may appear to be a strange omission, in actual fact it demonstrates a clear separation between civilian *cybersecurity* policy and military *cyberdefense* strategy. Both of these fields work in parallel to one other to advance French digital security, even though the MoD is subordinated to the Prime Minister who directs ANSSI. The only point on which the two strategies converge is on international cooperation and the need to support research, innovation and education. This presents a picture of a civilian-led framework for cybersecurity and cyberdefense in general.

The three documents which comprise French cybersecurity and cyberdefense policy primarily focus on defensive cyber capabilities and make little mention of offensive tools. The operational measures set out in the Pact of Cyber Defense and the National Digital Security Strategy focus primarily on strengthening the security and resilience of digital systems (hardware and software) and concentrate less on active defense. Details regarding French offensive and active capabilities can be found in other sources. France's Defense Minister confirmed in interviews that France does indeed possesses offensive cyber capabilities and, according to the military doctrine of 2014, cyberweapons should and could be used as support for conventional forces or in response to a conventional attack (Barluet, 2016; Cabirol, 2015). Such response options to cyberattacks were mentioned only in the Strategic Review of 2017, which focuses offensive capabilities within a military, defense-focused sphere.

Nevertheless, the emphasis of all the relevant strategy documents is on maintaining France's sovereignty. This is to be achieved through two goals. First, state technological capabilities and the ability to effectively and accurately process information must be preserved. Second, the ability of the state to access that information and communicate it effectively in order to be able to make decisions must also be ensured.

This focus on sovereignty is also reflected in the broadened conceptualization of digital security established in the National Digital Security Strategy. This conceptualization is one which encompasses both technical *and* non-technical aspects of cyber and French plans to develop domestic cybersecurity technologies and solutions in order to gain in autonomy and preserve that sovereignty.

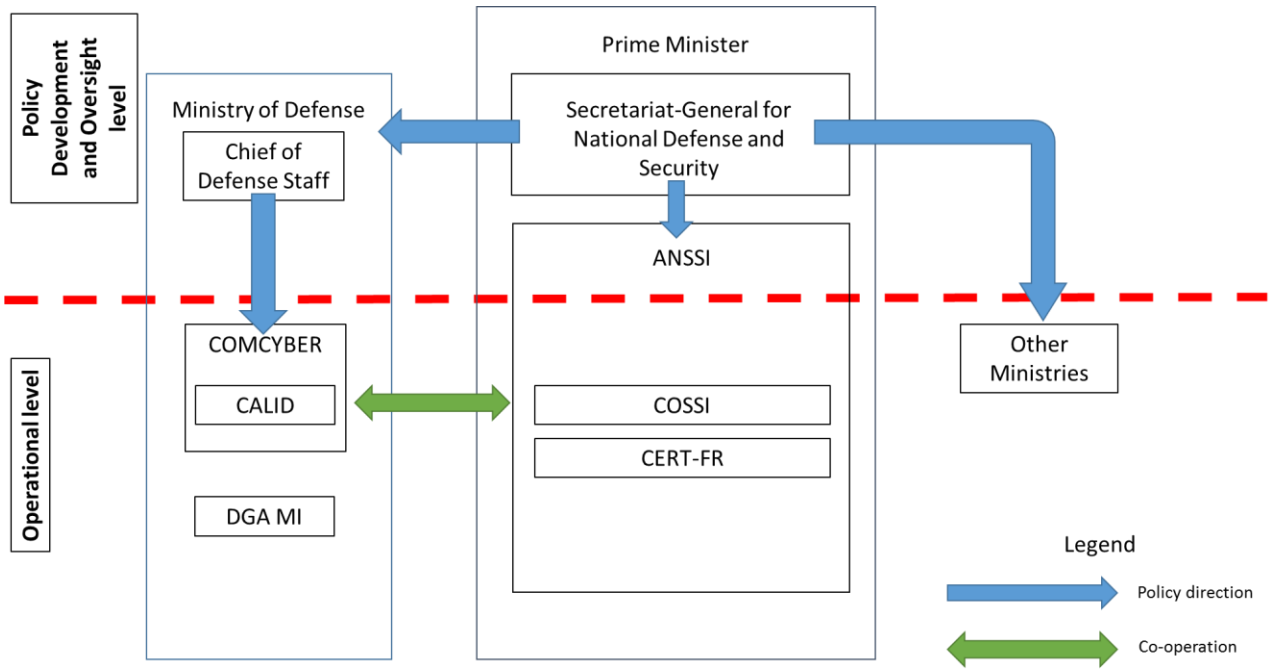
The wording adopted by the National Digital Security Strategy of 2015 and the Strategic Review of 2017 – the use of "digital" rather than "cyber" – demonstrates the willingness to broaden the understanding of cybersecurity issues and marks a shift in French strategic discourse, even in the field of defense policy. It shows a desire to shift from a restrictive *cyberwarfare* approach to a broader *information* warfare approach that also encompasses influence campaigns. In doing so, France has enlarged its scope of "cyber" action in general.

3. Current public cybersecurity structures and initiatives

3.1. Overview of national organization framework (key actors)

Diagram FR3 below provides a graphical representation of the organization of the French cybersecurity apparatus.

Diagram FR3: Oversight Organigram



3.2. National cybersecurity structures and initiatives: organization, mandate, legal aspects, operational capabilities

3.2.1. National Cybersecurity Agency (ANSSI)

The French cybersecurity and cyberdefense framework is separated between policy development and operationalization, as shown in Diagram 2 above. For cybersecurity (NOT cyberdefense) the **National Cybersecurity Agency (ANSSI)** is the lead agency operationalizing cybersecurity policy. This is a different positioning of leadership to other states such as the UK and Germany, where overall leadership is based in the policy-development entities.

ANSSI was created in 2009 after the White Paper of 2008 recommended the creation of a central agency dedicated to cybersecurity. On establishment, ANSSI was positioned under the aegis of the Prime Minister's office and reports to the Secretariat-General for National Defense and Security. ANSSI employs approximately 500 agents and is planning to increase this number to 600 by the end of 2017. It is based in Paris but also has 12 regional offices.

ANSSI's mandate is to:

1. Centralize, coordinate, prepare cybersecurity topics and assist state authorities on cybersecurity issues.
2. Provide help, support and information for enterprises to develop and implement the secure use of their information technology systems. ANSSI ensures that operators of critical infrastructures secure their IT systems according to the Military Program Law of 2013, which comprises 20 rules defined by ANSSI.
3. Protect France's sovereignty and autonomy in taking decisions by recruiting the right scientific, technical and operational experts.
4. Protect individuals by developing awareness campaigns and education programs on cybercriminality.

ANSSI also cooperates with the Ministry of Europe and Foreign Affairs by participating in information exchanges with approximatively 40 countries and in promoting the French model of cybersecurity.

3.2.2. Operational Centre for Information Systems Security (COSSI)

The **Operational Center for the Security of Information Systems (COSSI)** is a department of the ANSSI responsible for analyzing cyberthreats 24/7, identifying vulnerabilities in current systems, investigating ongoing attacks, defining possible response strategies, and supporting the implementation of urgent technical corrections on systems. COSSI includes a center responsible for monitoring and responding to cyberthreats 24/7 and alerting authorities. It is located in Paris and employs approximately 50 agents, a number which can be extended to 80 during major crises.

COSSI hosts the Computer Emergency Response Team-France (CERT-FR), which is part of the CERT international and European networks. CERT-FR contributes to international information exchanges on cyberthreats and vulnerabilities.

Due to its remit and expertise COSSI collaborates closely with its MoD counterpart, the Analysis Centre for Defensive Cyber Operations (CALID).

3.3. National cyberdefense structures and initiatives: organization, mandate, legal aspects, operational capabilities

3.1.1. Cyber Command (COMCYBER)

The Chief of the Defense Staff within the MoD supervises France's **Cyber Command** (**COMCYBER)**. This entity gathers all the cyberdefense units of the French armed forces and is headed by a Brigadier-General. It is a centralized Command that spans all military branches and is in charge of conducting military cyberoperations. COMCYBER is tasked with conducting cyber-intelligence, cyberdefense and cyberoffense operations within the legal framework of the international laws of armed conflicts and the French criminal and defense laws.

COMCYBER is composed of approximately 2,600 military personnel supported by around 600 experts from the IT section of the Directorate General of Armaments[9] (DGA) department of the MoD. From the time of writing to 2019, COMCYBER aims to recruit approximately 4,400 reservists who would serve as support troops in the event of a major cyber crisis (Establier, 2017).

To achieve its responsibilities and goals in cyberdefense, COMCYBER assigns tasks to four particular bodies:

- The **Analysis Centre for Defensive Cyber Operations (CALID)** is the operational center of the MoD. Its role is to anticipate and continually monitor cyberthreats and direct cyberdefense responses. It is located in the same building as COSSI with which it collaborates closely (Ministère de la Défense, 2014b).
- The **IT Section of the Directorate General of Armaments (DGA MI)** is the expertise center of the DGA for electronic warfare, information systems, telecommunications and information security. The DGA MI is responsible for procurement, research and development in information technologies. It is located in Bruz in Bretagne near the Cyberdefense Centre of Excellence, with which it collaborates closely. In regard to cyberdefense, the DGA MI has a set of missions. These are:

    1. To provide expertise on, and anticipate, cyberthreats.
    2. To provide advice and support for cyberdefense.
    3. To develop and evaluate cybersecurity products.
    4. To evaluate cybersecurity issues in every armament program.
    5. To develop cryptologic solutions for the government's communications.
    6. To coordinate research and development in cyber issues with other Ministries, industries and academia (Ministère de la Défense, 2014b).

- The **807th Transmissions Company** is a cyberdefense unit, which can be deployed, in overseas operations. Its role is to detect cyber threats, protect information systems and operate cyberdefense response for conventional units in operations abroad (Establier, 2017).
- **Operational Cyberdefense Reserve (OCR)** role will be to assist cyberdefense military specialists and DGA MI personnel to rebuild networks and information system infrastructures after major cyber crisis (Drahi, 2015). The recruitment process for the OCR started in October 2016.

[9] Direction Générale de l'Armement

3.4. Context: key public organizational framework

As stated above, the French organizational structure for cybersecurity and cyberdefense is highly centralized and is consistent with France's wider political structure. Cybersecurity and cyberdefense are managed at the national level by the Prime Minister and the Ministries of Defense, Europe and Foreign Affairs, and Economy and Finance but the framework for these policy areas is highly centralized around the ANSSI. This centralized framework, while innovative for cybersecurity, is consistent with France's political history and organization. This centralization is also found in practical situations, such as the development of a hub in Bretagne dedicated to research, education and innovation in cyberdefense.

The fact that ANSSI answers directly to the Prime Minister highlights two important facts. First, it demonstrates that cybersecurity is a civilian policy area, given that policy development and leadership stems from a civilian organ of government. Second, ANSSI's position in France's cybersecurity organizational framework shows that cybersecurity is a key priority for the French government. The conceptualization and development of a cyber-reserve also shows this prioritization given that it aims at quickly supplementing the IT experts within the MoD and could be seen as a way to circumvent budgetary limitations and having an "on-demand" volunteer workforce.

Despite the civilian oversight inferred from the leading position of the Prime Minister's office, the reality is more complicated. Even though the MoD is subordinate to the Prime Minister, the organizational framework is arranged with two parallel structures operating simultaneously: a civilian structure led by ANSSI and a MoD structure led by COMCYBER. Both structures have their own priorities, goals and capabilities and only cooperate through COSSI and CALID. The shortcomings of such a structure are the increased risks both of operational redundancy (causing additional costs as everything is built twice) and a lack of cooperation, collaboration and/or exchange between the two structures. There is also a risk of rivalries developing between the civilian and the military structures over resources and incident responses. The need to have these two structures, however, is understandable as each focuses on a different issue: ANSSI centers its attention on civilian, non-military issues including cybercrime while COMCYBER protects the MoD's systems and networks and builds up offensive capabilities. Nevertheless, as differences between cybercrime and state-sponsored cyberattacks can be more blurred than in the physical world, cooperation between the two structures would need to be robust.

This blurring, as well as the positioning of a civilian operational agency in the lead for cybersecurity *and* defense, presents a challenge for placing French cyberdefense and cybersecurity capabilities on a spectrum between offense and defense. As is the case with, for example, the UK, France reserves the right to develop offensive cyber capabilities (as set out in the Strategic Review of 2017), ostensibly placing it in a more offensive posture. But the lead operational agency falls under the oversight of the Prime Minister's office, a civilian organ of government. The capabilities being developed seem more akin to tools of deterrence. That being the case, even though France is developing offensive capabilities, its overall posture is one of defense.

4. Current cyberdefense partnership structures and initiatives

4.1. Public-Private cyberdefense partnerships

Details of French public-private partnerships (PPPs) in the field of cybersecurity and cyberdefense is scarce. The 2011 Defense and Security of Information Systems Strategy planned a PPP framework for the MoD consisting of that ministry sharing information with its "preferred" partners and enabling it to verify their cybersecurity positions (Ministère de la Défense, 2014a). Non-military PPPs, at least those that do not concern the MoD are handled by ANSSI.

ANSSI sets mandatory cybersecurity standards that private partners operating critical infrastructures are required to implement at their own cost. ANSSI is entitled to conduct cybersecurity inspections and order the implementation of specific measures in times of crisis. This authority is highlighted in the strategy documents themselves. These state that the private sector is responsible for its own cybersecurity, but French state authorities can intervene as support in the event of a major cyber crisis (Secrétariat Général de la Défense et de la Sécurité Nationale, 2015). This presents greater clarity regarding the division of responsibility between the state and private entities than, for example, the UK, where this division is more ambiguous (see UK Chapter, Section 4.1).

4.2. International cyberdefense partnerships

French international cooperation is oriented primarily towards NATO and the EU. These are historic alliances in which France is heavily invested economically, politically and socially. However, France also seeks to develop bilateral cooperation frameworks with states in areas of strategic interests like the Middle East and the Pacific region (Ministère de la Défense, 2014a).

For cyberdefense in the international military and intelligence spheres, France favors NATO partnership and collaboration with the Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Tallinn. However, ANSSI – a non-military body of the French cybersecurity framework – is also involved in the CCDCOE and has signed a Memorandum of Understanding with the NATO Cyber Defense Management Board in 2011. It also participates in international exercises on cybersecurity organized by the CCDCOE. France also wants to develop and promote international Confidence Building Measures for cyberspace through NATO *and* the OSCE, further blurring the lines between civilian and military/defense policy development.

At the regional level, France favors the EU for economic and industrial cybersecurity cooperation. However, it also wants to promote cyberdefense issues within the EU Command and increase the collaboration with EU partners on cyberdefense, especially with Germany, UK, Estonia and Belgium. France already has developed a specific cooperation framework with Germany on cloud computing (Brangetto, 2015).

4.3. Cyberdefense awareness programs

In contrast to some other states being examined for this collected edition, France has published details on at least two cyberdefense initiatives.

4.3.1. Citizen Cyberdefence Reserve:

The Citizen Cyber Reserve has been in operation since 2012 and is composed of approximately 150 volunteers who prepare and conduct awareness campaigns for specific audiences (Ministère de la Défense, 2014b).

4.3.2. Awareness programs within each military branch:

Each military branch is responsible for organizing their own awareness campaigns on cyberdefense issues. To do this, each branch is required to organize an annual cybersecurity information day for their personnel (Ministère de la Défense, 2014a).

4.4. Cyberdefense research programs

The emphasis of French research programs is mainly on developing French-based cybersecurity technologies and solutions to avoid the security and dependency risks inherent in a reliance on foreign suppliers. The goal is to use the Cyberdefense Centre of Excellence in Bretagne to stimulate research, innovation and education in cybersecurity by increasing cooperation within the existing cluster of expertise in Bretagne. This gathers together the Saint-Cyr-Coëtquidan School, the DGA MI, the CALID Bretagne (regional cell of CALID), ETRS, ENSTA and the Ecole Navale. There

is also a drive to create cooperation with industrial partners for research on cryptology, the analysis of perpetrators of cyberattacks, methods of attacks, expertise on software and malware and software development.

DGA MI provides financial support for academic technical and social science research on cyberdefense. The "Plan Cybersécurité" is an industrial plan to stimulate in France the creation of projects for cybersecurity solutions and cyberattack detection systems. The French authorities actively promote home-grown cybersecurity technologies and research at the European and international levels (Ministère de la Défense, 2014a).

4.5. Cyberdefense education and training programs

France has undertaken several measures to improve education and training. Three chairs of cyberdefense have been established at particular schools throughout France: in 2013 at the Saint-Cyr-Coëtquidan School in Bretagne; in 2014 at the Ecole Navale, also in Bretagne; and in 2016 at the Ecole de l'Air in the south of France. The curriculum at these schools examines cyberdefense and crisis management.

Since the 1990s the Officer School of Transmissions (ETRS) in Rennes, Bretagne, trains approximately 800 students annually on IT security. Since 2015, 48 officers graduated from the program on active cyberdefense and crisis management. There are other education programs that are adapted to the MoD's more current needs. In 2015 the National School of Advanced Techniques (ENSTA) in Bretagne established the same active cyberdefense and crisis management program as the ETRS. ENSTA is a civilian higher education institution with several military education programs (Drahi, 2015).

The Cyberdefense Centre of Excellence in Bretagne (launched in 2014) established the curriculum for the active cyberdefense and crisis management program and developed a simulation platform for the program with the DGA MI and CALID.

Finally the MoD organizes annual exercises on cyberdefense for cyberdefense troops and cybersecurity issues are included in all the other military exercises (Ministère de la Défense, 2014b).

5. Annex 1: Policy Spectra

These sliding scales represent three policy spectra:

1. The extent to which policy development and management in cyberdefense and cybersecurity is centralized;
2. The extent to which these areas fall under civilian or military oversight and
3. Whether or not the state under examination has a defensive or offensive cyberdefense posture.

As set out in the introduction to this edition, a state's position on these sliding scales is derived from the analysis in the snapshots. For example, if a state concentrates a significant amount of policy development and implementation responsibility in only a few or a single entity, it is reasonable to conclude that that state operates a more centralized approach to cybersecurity and defense leadership. Similarly, if responsibility in these sectors is placed in the defense ministry then there will be a greater degree of military rather than civilian oversight, and if the possession of offensive cyberdefense capabilities is explicitly stated in the policy literature, a state can reasonably be said to maintain an offensive cyberdefense posture, even if specific capabilities and tools are not mentioned.

5.1. Centralization vs Decentralization of Leadership

Diagram FR4: Spectrum of Centralization vs Decentralization of policy development and management

Centralized control ----X---------- Decentralized control

5.2. Civil vs defense posture and oversight

Diagram FR5: Spectrum of Civilian-Defense cybersecurity posture and oversight

Civilian oversight ----------X---------- Defense

5.3. Offensive vs defensive capabilities

Diagram FR6: Spectrum of Offensive vs Defensive cyberdefense capabilities

Offensive----------X----------Defensive

6. Annex 2: Glossary of Terms and Key Definitions

Term	Definition
Classified information	Article 413-9 of the French Penal Code states that «processes, objects, documents, pieces of information, computer networks, computerized data or files whose disclosure or access would be prejudicial to national defense or would lead to the disclosure of a national defense secret» are subject to classification measures to restrict their distribution or access.
Cybercrime	Acts contravening international treaties and national laws, targeting networks or information systems, or using them to commit an offence or crime.
Cyberdefense	The set of all technical and non-technical measures allowing a State to defend in cyberspace information systems that it considers to be critical.
Cybersecurity	The desired state of an information system in which it can resist events from cyberspace likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible. Cybersecurity makes use of information systems security techniques and is based on fighting cybercrime and establishing cyberdefense.
Cyberspace	The communication space created by the worldwide interconnection of automated digital data processing equipment.
Information system	Organized set of resources (hardware, software, personnel, data and procedures) used to process and circulate information.
Information systems security	All technical and non-technical protective measures enabling an information system to withstand events likely to compromise the availability, integrity or confidentiality of stored, processed or transmitted data and of the related services that these systems offer or make accessible.
Operator of critical importance (OIV - Opérateur d'importance vitale)	Article R. 1332-1 of the French Defense Code states that operators of critical infrastructures are designated among the public or private operators cited in Article L. 1332-1 of the same code, or among managers of the organizations cited in Article L. 1332-2. An operator of critical infrastructure: exercises activities cited in Article R. 1332-2 and included in a critical sector; and manages or uses for this activity one or more organizations or works, one or more facilities, whose damage, unavailability or destruction due to malicious action, sabotage or terrorism would directly or indirectly seriously compromise the military or economic capabilities, the security or the survival ability of the nation or seriously threaten the lives of its population.
Resilience	In the field of computing, the ability of an information system to withstand a breakdown or cyberattack and return to its initial operating state after the incident (Agence Nationale de la Sécurité des Systèmes d'Informations, 2011).

7. Annex 3: Abbreviations and Acronyms

Abbreviation/Acronym	English	French
ANSSI	Cybersecurity National Agency	Agence Nationale de Sécurité des Sytèmes Informatiques
CALID	Analysis Centre for Defensive Cyber Operations	Centre d'Analyse de Lutte Informatique Défensive
CCDCOE	NATO Cooperative Cyber Defense Centre of Excellence	-
CERT-FR	Computer Emergency Response Team-France	-
COSSI	Information Systems Security Operational Centre	Centre Opérationnel de Sécurité des Sytèmes Informatiques
COMCYBER	Cyber Command	Commandement de Cyberdéfense
DGA MI	IT Section of the Directorate General of Armaments	Direction Générale de l'Armement Maîtrise de l'Information
DSSI	Information Systems Defense and Security Strategy	Défense et sécurité des systèmes d'information – stratégie France
ENSTA	Superior National School of Advanced Techniques	Ecole Nationale Supérieure de Techniques Avancées
ETRS	Military school of transmissions	Ecole des Transmissions
MoD	Ministry of Defense	Ministère des Armées
SNSN	National Digital Security Strategy	Stratégie Nationale pour la Sécurité du Numérique

8. Bibliography

Agence Nationale de la Sécurité des Systèmes d'Informations, 2011. Information systems defence and security France's strategy.

Bamat, J., 2017. France's Macron "to end state of emergency", but keep its anti-terror powers [WWW Document]. Fr. 24. URL http://www.france24.com/en/20170609-france-state-emergency-macron-police-powers-civil-liberties-terrorism (accessed 8.24.17).

Barluet, A., 2016. La France muscle sa cyberdéfense [WWW Document]. Le Figaro. URL http://www.lefigaro.fr/international/2016/12/12/01003-20161212ARTFIG00221-la-france-muscle-sa-cyberdefense.php (accessed 8.8.17).

Brangetto, P., 2015. National Cyber Security Organisation: France, National Cyber Security Organisation. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn.

Cabirol, M., 2015. "La lutte informatique offensive n'est pas un tabou" (Jean-Yves Le Drian) [WWW Document]. RP Def. URL http://rpdefense.over-blog.com/2015/09/la-lutte-informatique-offensive-n-est-pas-un-tabou-jean-yves-le-drian.html (accessed 8.8.17).

Drahi, J.-R., 2015. La Cybersécurité. Terre Inf. Mag. 2–12.

Establier, A., 2017. ITW SDBR du vice-amiral A. Coustillère, Officier Général Cyberdàfense au MINARM [WWW Document]. RP Def. URL http://rpdefense.over-blog.com/2017/05/itw-sdbr-du-vice-amiral-a.coustilliere-officier-general-cyberdefense-au-minarm.html (accessed 8.8.17).

French Foreign Ministry, 2014. France and NATO [WWW Document]. Fr. Dipl. URL http://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/france-and-nato/ (accessed 8.24.17).

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

Ministère de la Défense, 2014b. La cyberdéfense.

Ministère de la Défense, 2013. French White Paper Defence and National Security 2013.

Ministère des Armées, 2017. Revue Stratégique de Défense et de Sécurité Nationale.

Poncet, G., 2016. Budget militaire : la France dépensera plus que la Russie en 2017 [WWW Document]. Point Int. URL http://www.lepoint.fr/monde/budget-militaire-la-france-depensera-plus-que-la-russie-en-2017--12-12-2016-2089696_24.php (accessed 8.24.17).

Secrétariat Général de la Défense et de la Sécurité Nationale, 2015. French National Digital Security Strategy.

Finland

Sean Cordey
University of St. Gallen

Highlights/Summary:

1. Key national trends

Finland is an important international economic and European actor in the fields of ICT. As a soft power oriented country, it is developing its cyber expertise and capabilities in view of becoming a forerunner. Moreover, the growing sense of insecurity has led to an acceleration and intensification of Finland's international (cyber) defense engagements and cooperation, most notably with NATO.

2. Key policy principles

2.1. Cybersecurity

The Finnish cybersecurity approach is holistic, comprehensive and inclusive. It is geared toward fostering the cyber resilience, preparedness and awareness of all actors; private and public. Specifically, cybersecurity policies encompass *inter alia* critical information infrastructure protection, cybercrime prevention, international cooperation and the development of expertise.

2.2. Cyberdefense

There is no specific cyberdefense policy or document in Finland. However, objectives are explicitly formulated in the cybersecurity strategy and require the development of comprehensive cyberdefense capabilities (military intelligence, defense and offense measures) and cyber preparedness of the armed forces.

3. Key national framework

3.1. Cybersecurity

Finland's specific cybersecurity and cyberdefense framework reflects its national security framework. As such, the civilian government leads the policy-strategic dimension while operational responsibilities are decentralized to the respective ministries, agencies and actors. Nonetheless, its coordination and monitoring are centralized within the Security Committee, a body located within and chaired by the Ministry of Defense.

3.2. Cyberdefense

The Ministry of Defense is tasked with protecting its information infrastructures and developing its cyber capabilities. As such, its cyberdefense operational arm is the Finnish Defense Forces C5 Agency and its cyber division. The different military entities collaborate with their civilian counterparts in terms of R&D and situational picture.

4. Cyber International cooperation

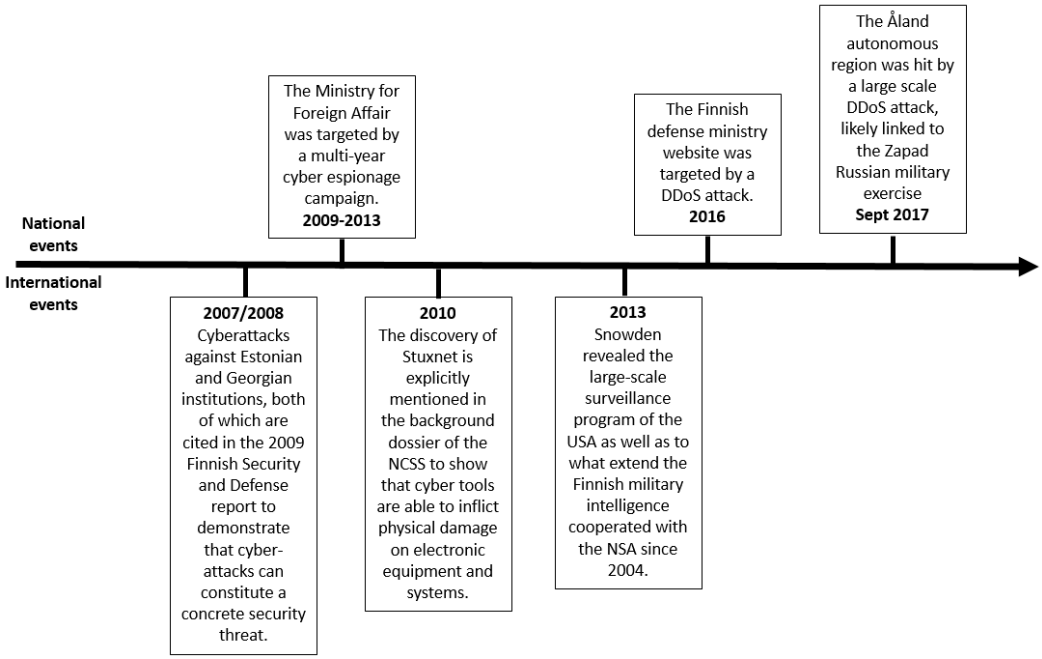
Finland's key international partners are its Nordic-Baltic neighbors (specifically NORDEFCO & NB8), the European Union (including the EDA, ENISA and cyber response teams) and – despite not being a member – NATO (through entities such as the CCDCOE, Hybrid CoE and cyberdefense exercises). Finland also pursue bilateral cyber cooperation with the United States.

1. Evolution of national cybersecurity policy (since mid-1990s):

1.1. Threat perceptions: trigger events

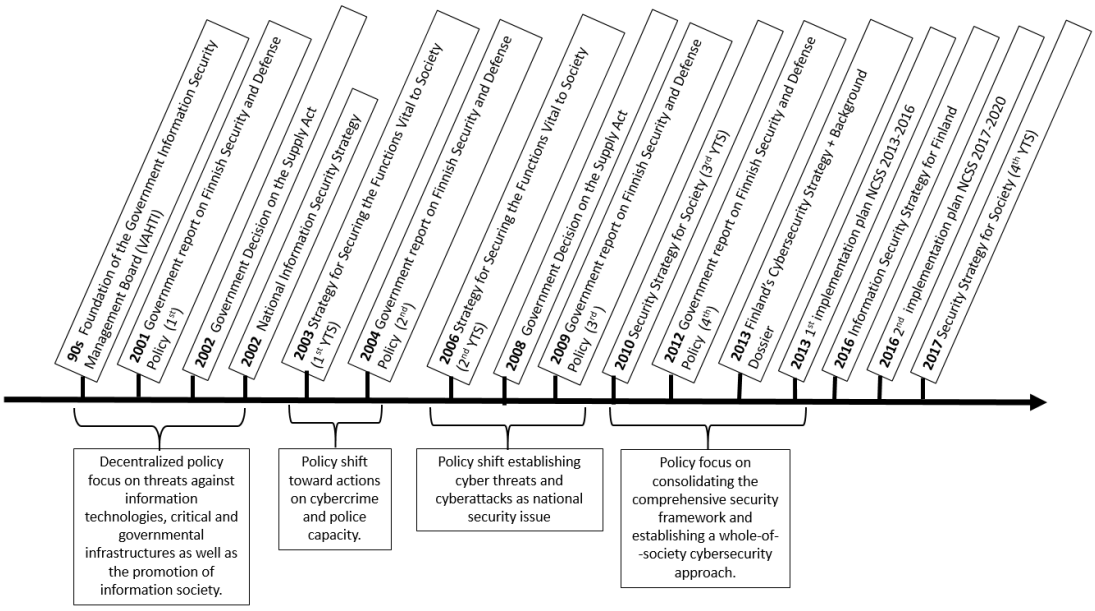
This sub-section describes the main domestic and international events that have had an impact on the shaping of cybersecurity and cyberdefense policies in Finland. It must be noted that no specific threats to Finland are explicitly mentioned in policy documents. However, the latest defense report recognizes that several cyber-attacks have targeted some Finnish critical infrastructures, industrial plants and political decision-making systems (Prime Minister's Office, 2017).

Diagram FN1: Timeline of trigger events



1.2. Main policy documents: key shifts in strategy

Diagram FN2: Timeline of policy developments and trends



1.3 Organizational structures: key parameters

Finland has a holistic approach to cybersecurity, which is focused on seizing the opportunities offered by digitalization and connectivity while mitigating emergent threats. As such, cybersecurity is fundamentally integrated into the national security framework[10]. Thus, its organizational structure reflects the existing separation of duties between the authorities and decentralized *modi operandi* relating to other security issues.

Political and strategic steering, provision of resources and operational preconditions are led by the civilian government, namely the Prime Minister, his office and the cabinet committee on foreign and security policy (UTVA[11]). The coordination of cybersecurity preparedness is led by the Security Committee (TK[12]), a body hosted and chaired by the Ministry of Defense (MoD), which also monitors the implementation and reviews of the National Cyber Security Strategy (NCSS).

Meanwhile, the civilian administrative branches are responsible for their own preparedness and cybersecurity related tasks. For instance, the Ministry of Transport and Communications (LVM) is responsible for safeguarding the functioning of electronic ICT systems. Meanwhile, the Ministry of Finance (MoF) is responsible for safeguarding the state administration's IT functions, information security and the service systems common to the central government (Secretariat of the Security and Defense Committee, 2013b). In parallel, the Finnish Defense Forces (FDF) are tasked with the development and maintenance of their own networks as well as cyberdefense/offense capabilities.

Overall, operational capabilities and strategic leadership is divided between civilian and military authorities, but with a weighting toward a military oversight through the TK. Nonetheless, the general process remains highly collaborative and consensual, aimed at bringing together all the civilian, military and private sector parties involved.

1.4. Context/Analysis: key national trends

Geopolitically, Finland is a neutral, non-nuclear parliamentary democracy[13], which makes use of considerable soft power over a wide range of issues (i.e. climate change, digitalization, education, culture, human right to development aid). Despite being located on the fringe of Europe, it has positioned itself as an important and proactive player in Nordic, European and international affairs. As such, it is a very active member of the EU and other regional organizations, such as the Organization for Economic Co-operation and Development (OECD), the Organization for Security and Co-operation in Europe (OSCE) or the Council of Europe (CoE). At the regional level, it remains strongly interconnected and dependent, for its energy[14] and trade, to its neighbors, most notably Russia. This situation is directly reflected in its foreign and defense policy, which is focused on balancing its relations and cooperation between the West and Russia while proactively promoting appeasement. Such a geopolitical arrangement is also found in Finland's non-aligned military defensive posture as well as its model of total defense, comprehensive security and preparedness.

Since the Ukraine crisis, Finland's insecurity perception has increased due notably to the deterioration of the security situation in Europe and in the Baltic Sea region as well as to the emergence and intensification of new security threats (i.e. hybrid threats, cyber threats, cyber espionage and more recently terrorism) has raised. In turn, this has led to the expansion of the budget allocated to defense, at its highest (2 872 million euro) since 2010 (Ministry of Defense, n.d.)[15]. In addition, it has also led to an acceleration of Finland's international defense (incl. cyberdefense) engagement and cooperation. For instance, despite not being a member of NATO, Finland, through its Partnership for Peace (PfP), closely cooperates with NATO on education, training or military capabilities development. In addition, it has in the past contributed to several NATO-led peacekeeping operations and missions (e.g. Afghanistan, Kosovo, Bosnia and Herzegovina). Currently, Finnish forces are part of the Resolute Support mission in Afghanistan.

Economically, Finland has a GDP per capita similar to that of France or the United Kingdom (International Monetary Fund, 2018). It has become a leader in the fields of information and communication technologies (ICT) and the digital industry, ranking third and second in the knowledge economy index and the networked readiness index respectively (The World Bank, 2012; World Economic Forum, 2016). Early on, the Finnish government has made efforts to harness the economic and social benefits of digital technologies. It has been very active in promoting and securing an information society and economy. As such, the protection of information, its systems and other digital assets as well as

[10] This is set out in the Security Strategy for Society, aka YTS.

[11] Valtioneuvoston ulko- ja turvallisuuspoliittinen ministerivaliokunta.

[12] Turvallisuuskomitea, founded in 2010 and regroups all the ministries and interested parties relating to security issues.

[13] Finland is a unitary state organized on a decentralized basis with three levels of governance: national, regional and local. As such, the local self-government principle is enshrined in the Constitution. It is also a federal state as the Aland Islands have been granted a special autonomous status.

[14] "Finland imports all of its natural gas and more than 90 percent of its oil and coal from Russia, meaning that around half of the country's energy use is dependent on its eastern neighbor" (Reid Standish, 2016).

[15] Although, it must be noted that in terms of share of GDP it is at its lowest (1.23% in 2018 vs. 1.46% in 2010). Furthermore, when considering the share of defense spending to the central government expenditure has been relatively stable ~ 5.0% since 2013.

the development of expertise have been seen as key to guarantee the development of its business environment and support Finland's economic and social model.

Overall, these geopolitical and economic dynamics have been key drivers for Finland's holistic approach to cybersecurity, which emphasizes not only soft power, international collaboration and economic interests but also defense and cyberdefense capabilities. Cybersecurity has thus come to be viewed as a key pillar to guarantee the prosperity of Finnish society and its welfare state in the short, medium and long term.

In addition, it is interesting to note that Finland's cybersecurity and cyberdefense policies have become increasingly integrated into the national security framework as awareness of new security threats and opportunities became apparent, for instance after the Snowden, Stuxnet and foreign ministry cyber-espionage cases. Indeed, before the 2010 Security Strategy for Society (YTS 2010[16]) and the 2013 NCSS, information security, cyberdefense, critical information infrastructure protection and the promotion of digital industry had instead operated in their respective silos.

3. Current cybersecurity policy

3.1. Overview of key policy documents

3.1.1. Security Strategy for Society 2017

The most recent document that sets out Finland's national security policy is the Security Strategy for Society 2017 (YTS 2017). This document is an overarching interdepartmental strategy that lays out the general principles and tasks relating to the governance and implementation of *preparedness*, *comprehensive security* and crisis management. Two concepts according to which the vital functions of society are to be jointly safeguarded by the authorities, business operators, organizations and citizens (Prime Minister's Office, 2013). Specifically, there are seven vital functions mentioned:

1. Management of Government affairs
2. International activity
3. Finland's defense capability
4. Internal security
5. Functioning of the economy and infrastructure
6. The population's income security and capability to function, and
7. Psychological resilience to crisis

With regard to cybersecurity, the YTS 2017 builds on its previous iteration (YTS 2010), which considered "Disturbances in the telecommunications and information systems – cyber threats" (Finnish Ministry of Defence, 2010) as a prime threat to the continuity of the above-mentioned vital functions. In addition, the strategy lists a number of cyber and information domain risks that the relevant ministries should address. These include, *inter alia*, cybercrime, data (information) security, energy supply and systems, telecommunication networks (public and private) as well as the continuity of the financial sector, food supply, transports and other public services operations (e.g. hospitals, courts). However, in comparison to the YTS 2010, the new document does not explicitly call for a greater military cyberdefense preparedness, instead, it underlines multifaceted threats and the need for a better situational picture (Security committee, 2017). For more details and measures, the strategy refers directly back to the European Network and Information initiative (NIS) and the 2013 NCSS.

3.1.2. National Cybersecurity Strategy 2013

Finland's 2013 Cybersecurity Strategy (NCSS) is the first national strategy dedicated to cyber. It was devised by the Security and Defense Committee[17] as part of the implementation plan of the YTS 2010. As such, it lays down Finland's vision, approach and strategic guidelines for cybersecurity within the existing framework and process of *Comprehensive Security* and *Security of Supply*[18].

A background dossier considers in more detail the actors relevant to the strategic guidelines as well as the cyber domain, its rapid development and potentially ensuing threats. Moreover, the dossier describes the principles of cybersecurity management and disturbance control arrangements as well as the provisions related to cybersecurity

[16] Yhteiskunnan turvallisuusstrategia.

[17] Predecessor of the Security Committee (TK), which operated under the MoD.

[18] Cf. 2013 Government resolution on security of Supply, which defines the focus areas and goals for the security of supply.

(Secretariat of the Security and Defence Committee, 2013a). These two documents are complemented by implementation plans that devise a series of concrete measures and are revised every three years. The first one was issued in 2014 while the second one in 2017. The strategy and related measures are addressed in some more details in the next section.

3.2. National cybersecurity strategy: fields, tasks, priorities

The 2013 NCSS is a comprehensive and inclusive strategy intended to foster national cyber preparedness while making Finland a leading country in cybersecurity. The strategy, alongside its background dossier, covers a broad range of topics and establishes the policy-development, oversight, hierarchy and ministerial responsibilities relating to cybersecurity. Moreover, it set out Finland's core visions for cybersecurity:

1. Finland can **secure its vital functions against cyber threats** in all situations.
2. Citizens, the authorities and businesses can effectively **utilize a safe cyber domain** and the competence arising from cyber security measures, both nationally and internationally.
3. (By 2016)[19] Finland will be a **global forerunner in cyber threat preparedness** and in managing the disturbances caused by these threats.

To achieve this vision, the documents underline the following 10 strategic guidelines or action fields upon which the implementation plans develop specific measures (Secretariat of the Security and Defence Committee, 2013a):

1. Create an efficient collaborative model between the authorities and other actors for the purpose of advancing national cybersecurity and cyberdefense
2. Improve comprehensive cybersecurity situation awareness among the key actors that participate in securing the vital functions of society
3. Maintain and improve the abilities of businesses and organizations critical to the vital functions of society as regards detecting and repelling cyber threats and disturbances that jeopardize any vital function and their recovery capabilities as part of the continuity management of the business community
4. Make certain that the police have sufficient capabilities to prevent, expose and solve cybercrime
5. The Finnish Defense Forces will create a comprehensive cyberdefense capability for their statutory tasks
6. Strengthen national cybersecurity through active and efficient participation in the activities of international organizations and collaborative fora that are critical to cybersecurity.
7. Improve the cyber expertise and awareness of all societal actors
8. Secure the preconditions for the implementation of effective cyber security measures through national legislation
9. Assign cyber security related tasks, service models and common cybersecurity management standards to the authorities and actors in the business community
10. The implementation of the Strategy and its completion will be monitored

In particular, the main measures of the implementations plans are the establishment of the Cybersecurity center (NCSC-FI) and its activities, the development of 24/7 information security operations of the government, a security network for encrypted data transfer, police responding capabilities, R&D and changes in legislation.

3.3. National cyber defense strategy: fields, tasks, priorities

Finland does not have any dedicated cyberdefense document or strategy. Nonetheless, cyberdefense goals and measures are formulated in the 2013 NCSS and its implementation plans. In particular, the strategy requires that the Finnish Defense Forces (FDF) develop and maintain comprehensive cyberdefense capabilities and cyber preparedness in order to pursue its statutory mandate[20], namely to protect the territorial integrity and national defense of Finland.

More specifically, the NCSS defines cyberdefense capabilities as encompassing at least two elements: military intelligence and proactive measures, whether defense or counter-attacks techniques (Secretariat of the Security and Defence Committee, 2013b). Thus, the armed forces are charged with developing and maintaining military cyber

[19] The time limit has been extended indefinitely in the 2017 implementation plan but was originally planned for 2016 in the NCSS.

[20] As defined in the Finnish Defense Forces Act.

situational awareness, developing and planning cyber warfare operations and protecting and monitoring its own networks in such a manner that they can carry out their statutory tasks irrespective of the threats in the cyber world. The FDF are also responsible with cooperating and supporting (in time of crisis) the other authorities, the businesses community and scientific community (Secretariat of the Security and Defence Committee, 2013b).

Regarding international cyberdefense cooperation, the NCSS explicitly refers to the possibility of bilateral and multilateral collaboration in order to facilitate the exchange of information between different actors and, in particular, to develop domestic capacities and harmonizes procedures. As such, it mentions the Nordic Defence Cooperation (NORDEFCO), the EU Military Staff, the European defense Agency (EDA) and NATO as key international partners.

3.4. Context/Analysis: key policy principles

Finland's cybersecurity policy is steered, owned and led by civilian authorities, namely the government, the UTVA and the president. The operational authority, however, rest in the hands of the ministries according to their respective tasks. Meanwhile, its coordination and monitoring are under the auspice of the TK, a body chaired by a military officer[21] (a major General) and hosted by the MoD but who regroups all the concerned security actors, whether governmental, private or from the civil society. Cybersecurity thus explicitly follows the comprehensive and all-of-society security approach laid out in the YTS 2010. As such, it is based on a strong collaborative model encompassing and recognizing the roles and responsibilities of both the civilian and military authorities but also that of the business community, academia and citizens.

With regard to cyberdefense, it is developed as an integral component of the Finnish comprehensive security and cybersecurity frameworks. The military is thus considered a key pillar for society's cybersecurity preparedness and operates closely alongside (and supports) the civilian cybersecurity bodies. Furthermore, the FDF cyberdefense tasks are explicitly acknowledged and described in the civilian policy documents. They comprise, *inter alia*, intelligence, surveillance as well as offensive and defensive cyber operations. A consequence of this inclusive approach is that there seems to be little need nor willingness for a separate and parallel cyberdefense strategy.

In addition, Finland's conception of the cyber domain reflects a certain duality in its approach to cyber, namely as an opportunity but also as a security issue. Indeed, on the one hand, the NCSS defines it as "an electronic information (data) processing domain comprising of one or several information technology infrastructures" (Secretariat of the Security and Defense Committee, 2013a), emphasizing it as a domain vital and critical to Finland's economic, social and international interests. On the other hand, the strategy also explicitly mentions the threat of cyberwarfare and the development cyberdefense capabilities. The last Government Defense (2017) report even "calls for the ability to carry out land, maritime, air and cyberspace operations", thereby considering it as its 4th domain of war[22]. Therefore, while integrated within each other, it seems as if the two conceptions tend to operate in their respective silos, with the civilian side underlining the opportunities and the military the security threats.

The overarching cybersecurity strategy is presented in Finland's NCSS, the background dossier and the implementation plans. Together, these documents set out Finland's triple vision for cybersecurity, namely: to safeguard vital functions; to guarantee a safe cyberspace; and to become a global cybersecurity forerunner. Concerning the last vision, one can consider that Finland is on the good track of becoming one of the leading countries in terms of cybersecurity preparedness. Indeed, if one refers to the 2017 International Telecommunication Union's (ITU) Global Cybersecurity index, Finland ranked 16th[23] (ITU, 2017). It is also the fourth most cyber secure country in the world according to the National Cybersecurity Index (e-Governance Academy, n.d.) and has one of the cleanest networks worldwide according to the 2016 Microsoft Security Intelligence report (Microsoft, 2016).

As mentioned above, the policy documents focus on different measures to guarantee Finnish cybersecurity preparedness and foster its national cyber resilience. These notably include the development of defensive capabilities, the development of expertise, the improvement of governmental information security infrastructure as well as the increase of international cooperation whether economic, diplomatic or military. In terms of international comparison, the scope is, apart from the cyberdefense capabilities, very comprehensive and similar to its European counterparts as well as the European Union cybersecurity strategy.

What is nonetheless prevalent in these measures is that Finland's government and policy-makers are aware of its small-state limitations, whether in resources, expertise or manpower. As such, they cannot, nor do they try to replicate what big cyber powers are pursuing (i.e. USA, Russia or China[24]). Instead, the focus is put on the efficient utilization, maximization and promotion of the existing public/private expertise and capabilities that are present nationally. In

[21] The chairman, however, has no direct executive authority on the other representatives and ministries.

[22] It is interesting to note that this takes place one year after NATO established cyberspace as a new domain of war.

[23] While technically loosing eight places in the ranking compared to the 2015 iteration, Finland actually gained six places if ones considers countries having similar ranks.

[24] For instance, setting up a cyber command or a centralized expert cyber center.

addition, collaboration with other states and organizations is emphasizes as crucial to further develop their own capabilities.

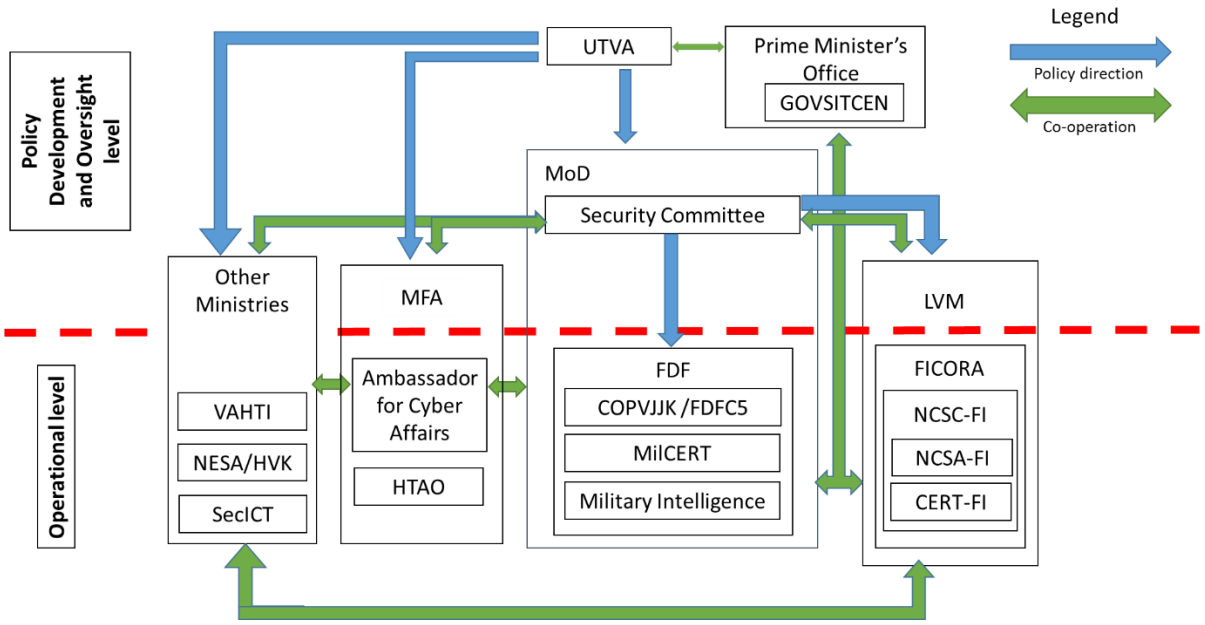
All the current policy documents published between 2013 and 2017 are highly interconnected and make explicit reference to each other, demonstrating how integrated and holistic the comprehensive security strategic structure is. For instance, the NCSS is referenced in other security policy documents, such as the 2012 Government report on Finnish Security and Defense, the 2017 Government Defense report, the YTS 2017 but also in the Sipilä's Government Program 2017-2019. In addition to being an integral part of the national security framework, the NCSS also supports and plays into other policy frameworks, such as the 2010 European Digital agenda, the European NIS Directive or Finland's digital agenda.

3. Current public cybersecurity structures and initiatives

3.1. Overview of national organization framework

Diagram FN3 below provides a graphical representation of the organization of Finland's cybersecurity apparatus.

Diagram FN3: Oversight organization



3.2. National cybersecurity structures and initiatives: organization, mandate, legal aspects, operational capabilities

3.2.1. The Finnish Government

3.2.1.1. The Cabinet Committee on Foreign and Security Policy

The government is the main actor responsible for the political and strategic steering of cybersecurity (Secretariat of the Security and Defence Committee, 2013a). Its other tasks relate to the provision of resources and the clarification of the operational precondition for the implementing the strategy.

The highest authority with regard to cybersecurity within the government is the **Cabinet Committee on Foreign and Security Policy (UTVA)** which is tasked with preparing and discussing any important aspects of foreign/internal security policy, national defense and other matters concerning Finland's international relations (Ministry of Defense, n.d.) . The committee meets regularly with the President of the republic and is chaired by the Prime Minister. In addition, its membership includes the Minister of Foreign Affairs, the Minister of Defense and a maximum of four other ministers depending on the issue. In the case of cybersecurity, these normally involve the Minister of Finance and the Minister of Transport and Communication.

3.2.1.2. The Government Situation Center

Hosted by the Office of the Prime minister, the **Government Situation Center (GOVSITCEN)** is a body responsible for the situational awareness of the Government (Prime Minister's Office, n.d.). As such, it compiles, synchronizes and disseminates a comprehensive, integrated and real-time security picture. This encompasses the combined situation picture compiled by the Cybersecurity Centre (NCSC-FI) and other bodies related to information-gathering (i.e. military, police, border intelligence) as well as the different administrative branches' estimates of the consequences of cyber incidents to society's vital functions (Secretariat of the Security and Defence Committee, 2013a).

3.2.2. Ministry of Defense

This section focusses solely on the Ministry of Defense (MoD)'s input into cyber***security*** in Finland. The MoD necessarily also has an important role to play in cyber***defense*** which will be examined in section 3.3 of this Snapshot.

3.2.2.1. The Security Committee

The **Security Committee (TK)**, established in 2013 within the MoD, is the successor to the Security and Defense Committee. It is a "permanent and broad-based cooperation body for proactive contingency planning within the government and ministries" (The Security Committee, n.d.). As such, it is not a cyber-specific body but rather focuses on Finland's comprehensive security. Chaired by a representative of the MoD, it includes 19 members and 3 experts from nearly all the administrative branches, authorities and business communities[25]. Its mandate is fourfold:

1. To contribute to the preparedness of comprehensive security and its coordination
2. To monitor and evaluate Finland's security and defense policy environment and societal changes and their impacts on comprehensive security arrangements
3. To monitor the activities of different administrative sectors and levels to maintain and develop comprehensive security arrangements
4. To coordinate, if necessary, large and significant preparedness-related issues, such as national coordination of preparedness, development of forms of cooperation, operational models, research and training

Furthermore, in addition of being responsible for the YTS 2017, which coordinates preparedness measures by the state, municipalities, organizations and the business community in various security situations (The Security Committee, n.d.), the committee is responsible for the coordination, joint monitoring, development and implementation of the NCSS. As part of this task the committee investigates for any duplication, identify any shortcomings, evaluates the effectiveness of the measures that have been implemented and creates the preconditions for coordinating the required action and needs between different actors (The Security Committee, 2014). In addition, it prepares the implementation plans, drafts annual reports for the Government on the state of cybersecurity preparedness, issues recommendation on its further development as well as monitor the effectiveness of cybersecurity exercises.

According to the 2017-2020 implementation plan, the TK will also host the **Finnish Cybersecurity Forum,** an exchange and cooperation platform between the academia, the public administration, the businesses and NGOs. Discussions will serve as a basis to analyses the up-to-datedness and progress of the NCSS's, its implementation programs and Finland's cybersecurity situation in general.

3.2.3. Ministry of Transports and Communication

3.2.3.1. The Finnish Communications Regulatory Authority

The Finnish Communications Regulatory Authority (FICORA) is the authority responsible for the steering and supervision of the reliability and security of electronic communications networks and information society systems (The Finnish Communications Regulatory Authority, 2015). It was established in 1988 as the Telecommunications Administration Centre and functions under the LVM. Its missions include, *inter alia*, the promotion of the information society in Finland, the publication of technical regulations, standards and certification as well as the development of cybersecurity situational awareness. It also oversees the protection of privacy and data in electronic communications

[25] For a detailed list of member see : https://turvallisuuskomitea.fi/tk/index.php?option=com_content&view=article&id=28&Itemid=102&lang=en#members

in addition to promoting national and international co-operation in the field (Manuel Suter and Elgin Brunner, 2008). Under the terms of the 2013 NCSS, FICORA also hosts the new National Cyber security center (NCSC-FI).

3.2.3.2. The National Cybersecurity Center

The **National Cybersecurity Center (NCSC-FI)**, established in 2014 at FICORA, is Finland's national information security authority that supports the public bodies, the business community and other actors in maintaining and developing cybersecurity. The center was created by the merger of the functions and duties of the CERT-FI and the GOV-CERT with that of FICORA's National Communications Security Authority (NCSA-FI). According to the NCSS its mandate is the following:

1. Compile and disseminate the cyber security situation picture in close cooperation with its support network
2. Compile and maintain a cyber threat risk analysis, in conjunction with different administrative branches and actors
3. Support the competent authorities and actors in the private sector in the management of widespread cyber incidents
4. Intensify cooperation and support the development of expertise.

Specifically, to develop the integrated situation picture (published annually), the center closely collaborates with other public and business entities, such as the GOVSITCEN, the SecICT, the police, the military or critical infrastructure operators (The Security Committee, 2014). Moreover, it also cooperates with national and international CERT networks, such as FIRST and other representatives of trade and industry to prevent, detect, report and resolve security breaches and threats against networks. The center's NCSA duties include the responsibility for security matters related to electronic transfer and processing of classified information.

As a side note, the last implementation (2017) plan has noted that despite its successful establishment and operations, the center suffers from financial limitations and that extra investments in resources are needed to strengthen its activities.

3.2.3. Ministry of Foreign Affairs

The **Ministry of Foreign Affairs (MFA)** is responsible for the coordination of Finland's positions and representation in cyber related international forums, such as the UN, OECD, OSCE, the EU, the CoE or NATO (Secretariat of the Security and Defence Committee, 2013a). Within the ministry this falls under the responsibility of its **Ambassador for Cyber affairs**, the first of which was nominated in June 2014. Meanwhile, from an organizational perspective, cybersecurity is otherwise treated in a horizontal and decentralized fashion with each of the ten sub-sections of the ministry's political department responsible for cybersecurity only in their respective tasks or organization. In addition, the MFA acts as the National Security Authority (NSA), which ensure that international information security obligations are implemented (The Security Committee, 2014).

Furthermore, in April 2018, the MFA appointed a **Hybrid Threat Ambassador**, whose mission covers the development of cyber-threat-countering strategies to protect IT-networks and to help enhance Finland's profile in the international arena. As such, it will closely cooperate with the different concerned officials and agencies in Finland as well as serve as a liaison officer with the newly established European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).

3.2.4. Ancillary agencies and initiatives

In addition to dedicated cybersecurity agencies and bodies, there are several other governmental entities and projects which play a prominent role in Finland's cybersecurity framework. The most relevant for this analysis are the following:

- The **Government Information Security Management Board (VAHTI[26]),** under the ministry of Finance, is responsible for steering, developing, coordinating and harmonizing the central government information security[27] and cybersecurity guidelines. It works in close cooperation with the TK, the other ministries and agencies to support and facilitate cooperation in the development of e-government and electronic services in the state sector (Suter & Brunner, 2008). In 2017, the ministry updated its mandate to include other

[26] The julkisen hallinnon digitaalisen turvallisuuden johtoryhmä.

[27] See definition section for more details.

operational development in the field of artificial intelligences, robotic as well as digital processing and cryptology (Ministry of Finance, n.d.).

- The **Development Project for the Central Government 24/7 Information Security Operations (SecICT)** reports to the MoF and is tasked with managing serious and far-reaching information and cyber related incidents affecting the central government (The Security Committee, 2014). It was set up in accordance with the 2013 NCSS to develop supplementary functions for the situation picture system, notably concerning technical and administrative information from activities and critical ICT systems. As such, it closely cooperated and exchanges information with the NCSC-FI.
- The **National Emergency Supply Agency (NESA/HVK)** acts as the cross-administrative operative authority for the security of supply in Finland. In term of cybersecurity of supply and cyber-threats against the continuity of information and communication infrastructure, NESA analyses the risks, writes and disseminate reports, establishes guidelines and conduct trainings (Ministry of Employment and the Economy, 2013). In addition, it is also manages and allocates resources to the CYBER 2020 program, which is tasked with improving the cybersecurity of businesses critical to the security of supply.[28]

3.3. National cyberdefense structures and initiatives: organization, mandate, legal aspects, operational capabilities

3.3.1. Ministry of Defense

As mentioned in section 2.3, the MoD is responsible for Finland's cyberdefense preparedness, policy guidance and the development of military cyber capabilities. To operationalize policy, the MoD has delegated the key tasks to the following agency:

3.3.1.1. Finnish Defense Forces C5 Agency

Within the Finnish Defense forces (FDF), ICT and cyberdefense is organized under the Defense Command C5 Division[29]. Its operational arm is the **Finnish Defense Forces C5 Agency** (PVJJK[30]/FDFC5A), which was founded in 2007 with the fusion of the FDF IT Center and the National Defense Management Departments and IT centers. As such, it is led by a Colonel, operates in over 18 location across Finland, and is staffed with 400 people, mostly civilians. Organizationally, the agency is divided into the following four sections (The Finnish Defence Forces, n.d.):

1. **The Headquarters**, tasked with controlling and monitoring the FDF's technical systems and implements procurement
2. **The IT-Services Division**, tasked with providing services for operational information systems and integrating the acquired information and communications technology services into the Defense Forces
3. **The Communication and Information Service Divisions**, tasked with operational IT-support for management units, the training activities of the FDF and the maintenance of security technology
4. **The Cyber Division**, tasked with the protection of data networks and services, the development of cyber defense and the FDF's cyber situational awareness. In addition, it develops cyber defense anti-attack and detection mechanisms

PVJJK also cooperates with the Government ICT center (VALTORI) to produce and maintain its network services as well as with the NCSC-FI, with whom it exchanges information to draw the cyber situation picture. In the near future, its Director expects that the center will be strengthened in staff (The Finnish Defence Forces, 2018). For instance, some have advanced the need of 200 additional full-time cybersecurity specialists by 2024 (Gerard O'Dwyer, 2018). However, currently, it finds itself restricted financially and has trouble competing with the private sector in attracting cyber experts (Gerard O'Dwyer, 2018).

[28] The program has been granted 20 million euros and 10 persons for the 2016-2020 period. This, however, includes the resources that are already earmarked to the National Cybersecurity center.

[29] Johtamisjärjestelmäosasto

[30] Puolustusvoimien johtamisjärjestelmäkeskus

3.4. Context: key public organizational framework

The Finnish cyber architecture reflects the existing *modi operandi* of its national security approach devised in the Security Strategy for Society. As such, it is holistic, multilevel, horizontal and interdepartmental. Specifically, strategic political guidance and steering of cybersecurity is centralized in the hands of the civilian government, namely in the Prime Minister's Office and the UTVA. In addition, the coordination and monitoring of the NCSS is also centralized in the TK, a MoD body. However, the operational development and day-to-day tasks are highly *de*centralized, with each ministry responsible for its own cyber preparedness and the management of cyber related issues relevant to their statutory tasks. Therefore, despite this apparent policy centralization, most of the implementation power, capabilities and policy recommendations remain in the hands the ministries, of which the following four are the most pertinent: the MoF, LVM, MFA and the MoD.

That being the case reflects some sorts of administrative inertia. The responsibilities and roles in term of cybersecurity have naturally evolved from the pre-existing agencies, expertise, policies and mandates of each ministries. Thus, the NCSS has not created new competencies or a new framework *per se*, but is rather a compromise between the different ministries, integrating cybersecurity within the existing entities with the existing resources. An example of this is the NCSC-FI, the key actor and measure of the NCSS. It was founded by merging two pre-existing entities (the NCSA-FI and CERT-FI). At the same time as this merger, VALTORI's and NESA's roles and mandates were updated and reinforced. In addition, the organization has also been heavily influenced by foreign examples[31] – most notably the Netherlands and Denmark – from which the NCSC-FI was imported (Martti Lehto et al., 2017).

There are, however, some potential problems and shortcomings to such an approach. The first is that the operational decentralization as well as the unclear delimitation of tasks and responsibilities within the strategy and the implementation plans have led the different administrative sectors to operate solely within their respective silos. Every ministry has defined its own goals and has developed its own approach according to very different understandings, prioritization and resource allocation. In addition, the ministries tend to be very protective of their areas of activities, thus preventing the formation of any clear and strong cyber leadership. This lack of sufficiently strong and determined strategic management has not only hampered the implementation of the NCSS but also poses a critical problem should a large-scale cyberattack occur. Indeed, the existing framework provides no clear strategic direction in respect of which agency is responsible to coordinate and lead a defensive response in the wake of such an event (Gerard O'Dwyer, 2018). In response, a centralized Finnish Cyber Defense Command, that could be set up in the Prime Minister's Office, has been argued for in a 2017 report on the state of the NCSS (Martti Lehto et al., 2017)[32].

Finally, there seem to be a generalized imbalance between the NCSS's objectives/vision and the resources provided to reach it. Most of the key cyber bodies, whether civilians (NCSC-FI) or military (PVJJK) are suffering from the small financial contribution (Martti Lehto et al., 2017). This trend also applies to the domain of cyber R&D and the Finnish Funding Agency for Technology and Innovation (more details in section 4.4). For instance, the initial funding for the national cyber research agenda (aka. Cyber Trust) was first refused and later cut in half (DIMECC, 2017). This imbalance is unexpected given Finland's progress, perception and international reputation in global digitalization.

[31] i.e. European and small-states similar in stature to Finland

[32] This report was mandated by the Finnish Government and is only available in Finnish, see the sources for more details.

4. Cyberdefense and Cybersecurity partnership structures and initiatives

4.1. Public private cyberdefense partnerships

There is very little information in Finnish policy documents about any specific public private partnerships (PPPs) in the field of cybersecurity and cyberdefense. Nonetheless, **NESA** acts as a network of various PPP initiatives related to the security of supply, and as such to cybersecurity. Specifically, it supports public-private cooperation by developing continuity management tools for enterprises, providing associated training, organizing shared exercises for enterprises and public bodies as well as by steering the operations of the different sectors (National Emergency Supply Agency, n.d.).

Furthermore, the **Finnish Information Security Cluster** (aka. the cyber security cluster or FISC) acts as a national hub for PPP. It was established in 2012 as a non-profit organization by 50 important Finnish information security companies to promote their businesses and operations in national and international context. As such, it collaborates with key government agencies to produce studies, organize consultations and monitor the implementation of cybersecurity guidelines in order to foster cyber resilience, baseline requirement, good practices and information exchanges.

On the International level, Finland conducts cybersecurity-related cooperation with the **European Public-Private Partnership for Resilience (EP3R)**, which acts at the European level to develop a reliable control system for a resilient information and communication technology infrastructure (The Security Committee, 2014).

4.2. International Cyberdefense partnerships

Finnish international cyberdefense cooperation is primarily oriented toward regional cooperation trough the Nordic-Baltic axis, NATO and the EU framework. Specifically, northern efforts take place within **the Nordic Defense Cooperation (NORDEFCO)**, a cooperative structure between Denmark, Finland, Iceland, Norway and Sweden, which comprises both experts and decision-makers from the Nordic political and military establishment and whose explicit focus is, among others, cyberdefense. The primary objective for a unified Nordic approach to cyberdefense is to develop better joint cyber defense capabilities based on enhanced information sharing, identifying best-practice, computer emergency responses and regular cyber security-based defense exercises (Gerard O'Dwyer, 2017). The NORDEFCO members therefore conduct technical cooperation, joint cyber research, and serial training and cyber exercises. In addition, they have developed a joint CERT and MilCERT network to coordinate monitoring, detection, and response to cyberattacks as well as information exchange and other educational activities. Since September 2015, Nordic cyberdefense cooperation is also reinforced with the three Baltic States (3B) – Estonia, Latvia and Lithuania – after joint non-paper on enhanced Nordic-Baltic cooperation was signed.

Despite not being a member of the alliance, **NATO** is Finland's second key cyberdefense partner. As such, it closely cooperates with the alliance in the framework of its Partnership for Peace Program (PfP), Enhanced Opportunity Program (EOP) and more recently through its political framework agreement on cyberdefense[33]. According to these, Finland participates in NATO's multinational R&D programs (i.e. NATO's CCDCOE), cyberdefense exercises (i.e. Lock Shields 17 & 18) and other capacity building initiatives. In addition, it hosts and is a member of the newly established **European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).** The new center, under the auspices of the EU and NATO, is among other, tasked with developing advanced systems to improve civil-military capabilities, resilience and preparedness to counter hybrid threats with a special focus on Nordic and European security (Gerard O'Dwyer, 2017). It will also liaise with NORDEFCO and collaborate with NATO and EU-operated cybersecurity organizations.

As an EU member State, Finland cooperates with its European counterparts on issues of economic/industrial cybersecurity, cybercrime and cyberdefense. For instance, it actively participates and supports the works of the European Network and Information Security Agency (ENISA), the European law enforcement agency (Europol), Body of European Regulators for Electronic Communications (BEREC), the European Forum for Member States (EFMS), the EU Military Staff (EUMS) and the European Defense Agency (EDA). Moreover, Finland is joining by the end of 2018 the recently announced **EU Cyber Rapid Response Force** which operates under the new European Permanent Structured Cooperation.

Furthermore, Finland also cooperates bilaterally on cyberdefense, cybersecurity and cybercrime. Its biggest partner is the **United States**, with whom it has established a cyber-dialogue (alongside other Nordic and Baltic states) which covers topical issues relating to cyberspace, cybersecurity, international law, cyber domain standards and PPPs. In

[33] The agreement, signed in February 2018, provides a framework to improve situational awareness, compatibility, capabilities building, detection of cyber incidents and resilience to disruptions in information networks. It eases up exchange information and promote learning. Furthermore, Finland is the first PfP country with whom NATO has signed an agreement in the field of cyber defense.

addition, both countries have also conducted a bilateral cyberdefense exercise together in September 2017, the so called Cyber Lightning exercise (The Finnish Defence Forces, 2017). With regard to cybercrime, the Finnish police cooperates closely with the FBI.

On the international level, Finland also participates in a number of other cyber initiatives, most notably: the OSCE and its confidence building measures; the UN and the World Summit on the Information Society (WSIS); the International Telecommunication Union (ITU) and its Global Cybersecurity Agenda initiative; or with the Organization for Economic Co-operation and Development (OECD) and its international guidelines for cyber security.

4.3. Cyber defense awareness programs

The TK, alongside the Confederation of Finnish Industries, the MoF and some companies, organize each year, as part of the European Cyber Security Month (ECSM), a **National Information and Cybersecurity Week.** A week, during which an awareness campaign on cybersecurity and information security is pursued, by means of events and publications, for the citizens, companies and public servants (The Security Committee, 2016).

4.4. National cyber defense research program

As part of the NCSS's goal to improve research and competence in the field of cybersecurity and cyberdefense, Finland has established an interdisciplinary **Center of Cybersecurity Excellence and innovation** within the framework of its Strategic Centre for Science, Technology and Innovation in the Field of ICT (DIMECC[34]) in the city of Jyväskylä. The center is charged with conducting R&D and international cooperation to allow the development of a strong national cybersecurity cluster (The Security Committee, 2014).

In addition, on the military side, the FDF have, through their Defense Research Agency (DRA), set up a **national crypto laboratory** to overcome the existing shortcoming in cryptographic expertise (The Security Committee, 2014). As such, the DRA pursues other specific researches on cyber defense and electronic warfare systems (The Finnish Defence Forces, n.d.).

On the civilian side, Business Finland (TEKES[35]) and the Academy of Finland have, according to the NCSS, developed a **strategic research agenda** 2014-2017 for cyber (i.e. cyber trust[36]). The program brought together the academia and big corporation and was focused on technology resilience, awareness and security. In addition, they launched a joint R&D&I program (i.e. ICT 2023) focused on improving Finland's scientific expertise in computer science and digital content development. In addition to their own research Finnish universities and research institutes, such as the Technical Research Centre of Finland (VTT), also participate in large joint European cyber projects, such as the SASER Celtic Plus research program or the ECOSSIAN EU project.

4.5. Cyberdefense education and training programs

Very little information and details concerning cyberdefense education has been made public. Nonetheless, the implementation plan of the strategy (2014) mentions training at all level for the police as well as the defense forces. In addition, the **National Defense Training Association of Finland** has been organizing every year a cybersecurity curriculum open to all citizen and authorities (The Security Committee, 2016).

Finnish universities and polytechnic institutions, in particular that of Jyväskylä, Aalto, Oulu, Tampere and Helsinki, have also become key partners in the development of advanced cyber technical education, tools, and platforms for training exercises. In total, seven institutions have developed courses or programs for cybersecurity and cyberdefense.

[34] Aka. TIVIT or DIGILE

[35] Aka. the Finnish Funding Agency for Technology and Innovation or Innovaatiorahoituskeskus Tekes.

[36] In the recent years, cybersecurity and defense research have suffered severe budget cuts (DIMECC, 2017).

5. Annex 1: Policy Spectra

These sliding scales represent three policy spectra:

1. The extent to which policy development and management in cyberdefense and cybersecurity is centralized;
2. The extent to which these areas fall under civilian or military oversight and
3. Whether or not the state under examination has a defensive or offensive cyberdefense posture.

As set out in the introduction to this collection, a state's position on these sliding scales is derived from the analysis in the snapshots. For example, if a state concentrates a significant amount of policy development and implementation responsibility in only a few or a single entity, it is reasonable to conclude that that state operates a more centralized approach to cybersecurity and defense leadership. Similarly, if responsibility in these sectors is placed in the defense ministry then there will be a greater degree of military rather than civilian oversight, and if the possession of offensive cyberdefense capabilities is explicitly stated in the policy literature, a state can reasonably be said to maintain an offensive cyberdefense posture, even if specific capabilities and tools are not mentioned.

5.1. Centralization vs Decentralization of Leadership

Diagram FN4: Spectrum of Centralization vs Decentralization of policy development and management

Centralized control ----------X---------- Decentralized control

5.2. Civilian vs defense posture and oversight

Diagram FN5: Spectrum of Civilian-Defense cybersecurity posture and oversight

Civilian oversight ----------X---------- Defense

5.3. Offensive vs defensive capabilities

Diagram FN6: Spectrum of Offensive vs Defensive cyberdefense capabilities

Offensive----------X---------- Defensive

6. Annex 2: Key definitions

Term	Definition
Information Infrastructure	Information infrastructure means the structures and functions behind information systems that electronically transmit, transfer, receive, store or otherwise process information (data).
Critical Information Infrastructure	Critical information infrastructure refers to the structures and functions behind the information systems of the vital functions of society which electronically transmit, transfer, receive, store or otherwise process information (data).
Cyber	The word 'cyber' is almost invariably the prefix for a term or the modifier of a compound word, rather than a stand-alone word. Its inference usually relates to electronic information (data) processing, information technology, electronic communications (data transfer) or information and computer systems. Only the complete term of the compound word (modifier + head) can be considered to possess actual meaning. The word cyber is generally believed to originate from the Ancient Greek verb κυβερεω (kybereo) "to steer, to guide, to control".
Cyber risk	Cyber risk means the possibility of an accident or vulnerability in the cyber domain which, if it materializes or is being utilized, can damage, harm or disturb an operation that depends on the functioning of the cyber domain.
Cyber domain, Cyber environment	Cyber domain means an electronic information (data) processing domain comprising of one or several information technology infrastructures. Note 1 Representative to the environment is the utilization of electronics and the electromagnetic spectrum for the purpose of storing, processing and transferring data and information via telecommunications networks. Note 2 Information (data) processing means collecting, saving, organizing, using, transferring, disclosing, storing, modifying, combining, protecting, removing, destroying and other similar actions on information (data).
Cyber security	Cybersecurity means the desired end state in which the cyber domain is reliable and in which its functioning is ensured. Note 1 In the desired end state the cyber domain will not jeopardize, harm or disturb the operation of functions dependent on electronic information (data) processing. Note 2 Reliance on the cyber domain depends on its actors implementing appropriate and sufficient information security procedures ('communal data security'). These procedures can prevent the materialization of cyber threats and, should they still materialize, prevent, mitigate or help tolerate their consequences. Note 3 Cyber security encompasses the measures on the functions vital to society and the critical infrastructure which aim to achieve the capability of predictive management and, if necessary, tolerance of cyber threats and their effects, which can cause significant harm or danger to Finland or its population.
Cyberdefense[37]	The national defense related sector of cybersecurity, which incorporates the capabilities of intelligence, surveillance, cyber-attack and cyberdefense.
Information (data) security	Information security means the administrative and technical measures taken to ensure the availability, integrity and confidentiality of data.
Cyber threat	Cyber threat means the possibility of action or an incident in the cyber domain which, when materialized, jeopardizes some operation dependent on the cyber world. Note Cyber threats are information threats which, when materialized, jeopardize the correct or intended functioning of the information system.

[37] As defined in the Government's Defense Report of 2017.

7. Annex 3: Abbreviations

Abbreviation/Acronym	Finnish	English
BEREC	-	Body of European Regulators for Electronic Communications
CCD COE	-	NATO cooperative Cyberdefense Center of Excellence
CERT-FI	-	Finnish National CERT
CoE	-	Council of Europe
DDoS	-	Denial-of-service attack
DIMECC	-	Digital, Internet, Materials & Engineering Co-Creation
DSA	-	Designated security Authorities
ECSM		European Cyber Security Month
EDA	-	European Defense Agency
EOP	-	Enhanced Opportunity Program
EU	-	The European Union
FDF	Försvarsmakten	Finnish Defense Forces
FICORA	Viestintävirasto	The Finnish Communications Regulatory Authority
GDPR	-	General Data Protection Regulation
GOV-CERT	-	Government CERT
GOVSITCEN	-	Government Situation Center
HTAO	-	Hybrid Threat Ambassador's Office
Hybrid CoE	-	Centre of Excellence for Countering Hybrid Threats
ICT	-	Information & Communication Technologies
ITU	-	International Telecommunications Union
LVM	Liikenne- ja viestintäministeriö	Minister of Transport and Communication
MFA	Ulkoministeriö	Ministry of Foreign Affairs
MoD	Puolustusministeriö	Ministry of Defense
MoF	Valtiovarainministeriö	Ministry of Finance
MoI	Sisäministeriö	Ministry of the Interior
NATO	-	North Atlantic Treaty Organization

NB8	-	Nordic Baltic cooperation
NCSA-FI	-	Finnish National Communications Security Authority
NCSC-FI	Kyberturvallisuuskeskus	The National Cybersecurity Center
NCSS	Suomen kyberturvallisuusstrategia	National Cybersecurity Strategy
NESA/HVK	Huoltovarmuuskeskus	National Emergency Supply Agency
NIS	-	Network and Information initiative
NORDEFCO	-	Nordic defense Cooperation
NSA	-	National Security Authority
OECD	-	Organization for Economic Co-operation and Development
OSCE	-	Organization for Security and Co-operation in Europe
PfP	-	Partnership for Peace
PPP	-	Public Private Partnerships
PVJJK/FDFC5A	Puolustusvoimien johtamisjärjestelmäkeskus	Finnish Defense Forces C5 Agency
SecICT	-	Development Project for the Central Government 24/7 Information Security Operations
TEM	työ- ja elinkeinoministeriö	Ministry of Employment and the Economy
TEKES	Innovaatiorahoituskeskus Tekes	Finnish Funding Agency for Technology and Innovation
TIVIT/ DIGILE	-	Strategic Centre for Science, Technology and Innovation in the Field of ICT
TK	Turvallisuuskomitea	The Security Committee
UTVA	Valtioneuvoston ulko- ja turvallisuuspoliittinen ministerivaliokunta	Cabinet Committee on foreign and security policy
UN	-	United Nations
VAHTI	julkisen hallinnon digitaalisen turvallisuuden johtoryhmä	Government Information Security Management Board
VALTORI	Valtion tieto- ja viestintätekniikkakeskus	The Government ICT Center
WSIS	-	World Summit on the Information Society
YTS	Yhteiskunnan turvallisuusstrategia	Security Strategy for Society

8. Bibliography

DIMECC, 2017. The Finnish Cyber Trust Program 2015-2017 (No. 7). DIMECC, Helsinki.

e-Governance Academy, n.d. National Cyber Security Index [WWW Document]. Natl. Cyber Secur. Index. URL https://ncsi.ega.ee/ncsi-index/

Gerard O'Dwyer, 2018. Finland government examines centralised cyber defence. Comput. Wkly.

Gerard O'Dwyer, 2017. Nordic states deepen cyber defence collaboration. Comput. Wkly.

International Monetary Fund, 2018. World Economic Outlook Database, January 2018.

ITU, 2017. Global Cybersecurity Index (GCI).

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T., Salminen, M., 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi.

Microsoft, 2016. Microsoft Security Intelligence Report (No. 21). Microsoft.

Ministry of Defence, 2010. Security Strategy for Society - Government Resolution 16.12.2010.

Ministry of Defense, n.d. Share of Defence Budget of GDP [WWW Document]. URL http://www.defmin.fi/en/tasks_and_activities/resources_of_the_defence_administration/finances/share_of_defence_budget_of_gdp

Ministry of Defense, n.d. The Cabinet Committee on Foreign and Security Policy [WWW Document]. Minist. Def. URL https://www.defmin.fi/en/tasks_and_activities/defence_policy/actors_in_defence_policy/cabinet_committee_on_foreign_and_security_policy

National Emergency Supply Agency, n.d. The National Emergency Supply Agency [WWW Document]. URL https://www.nesa.fi/organisation/the-national-emergency-supply-agency/

Prime Minister's Office, 2017. Government's Defence Report.

Prime Minister's Office, 2013. Finnish Security and Defence Policy 2012. Government Report.

Prime Minister's Office, n.d. Situation Centre [WWW Document]. URL https://vnk.fi/en/situation-centre

Reid Standish, 2016. How Finland Became Europe's Bear Whisperer. Foreign Policy.

Secretariat of the Security and Defence Committee, 2013a. Finland´s Cyber security Strategy.

Secretariat of the Security and Defence Committee, 2013b. Finland's Cybersecurity Strategy: Background dossier.

Suter, M., Brunner, E., 2008. Critical Information Infrastructure protection, Finland, in: International CIIP Handbook 2008/2009. Center for Security Studies, Zurich.

The Finnish Communications Regulatory Authority, 2015. Information security services of the NCSC-FI [WWW Document]. URL https://www.viestintavirasto.fi/en/cybersecurity/ficorasinformationsecurityservices.html

The Finnish Defence Forces, 2018. Puolustusvoimien johtamisjärjestelmäkeskus juhlii vuosipäiväänsä 22.6. [WWW Document]. URL https://puolustusvoimat.fi/logistiikkalaitos/kumppanit?p_p_id=101&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_101_struts_action=%2Fasset_publisher%2Fview_content&_101_assetEntryId=8809399&_101_type=content&_101_urlTitle=puolustusvoimien-johtamisjarjestelmakeskus-juhlii-vuosipaivaansa-22-6-

The Finnish Defence Forces, 2017. Finland and the United States Training in Cyber Defence Together [WWW Document]. URL https://puolustusvoimat.fi/en/article/-/asset_publisher/suomi-ja-usa-harjoittelevat-kyberpuolustusta

The Finnish Defence Forces, n.d. Finnish Defence Forces C5 Agency [WWW Document]. URL https://puolustusvoimat.fi/en/about-us/c5-agency

The Finnish Defence Forces, n.d. About the Defence Research Agency [WWW Document]. URL https://puolustusvoimat.fi/en/about-the-research-agency

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

The Security Committee, 2014. The Implementation Programme for Finland's Cybersecurity Strategy.

The Security Committee, n.d. The Security Committee – operation and responsibilities [WWW Document]. URL https://turvallisuuskomitea.fi/en/the-security-committee-operation/

The World Bank, 2012. Knowledge Economic Index.

World Economic Forum, 2016. Networked Readiness Index.

Germany

Patrice Robin
Centre for Security Studies
ETH Zürich

Highlights/Summary

1. Key national trends

Germany is an important international economic actor and is developing an international presence in both cybersecurity and cyberdefense, primarily from a soft power perspective. This is being developed within the framework of its leadership position in the EU as well as its co-operation with partnerships such as NATO.

In terms of specific cybersecurity and cyberdefense frameworks, Germany is undergoing a period of centralization, with the policy development and leadership role being taken up by the Federal Ministry of the Interior (BMI) in cybersecurity, and the Ministry of Defense leading in cyberdefense. Germany is making statements about developing offensive cyber-capabilities under the aegis of its Ministry of Defense, but the lack of open-source data on these capabilities and the fact that overall strategic leadership sits with a civilian entity means that cybersecurity and cyberdefense remain predominantly civilian, socio-economic policy areas.

2. Key Policy Principles

2.1. Cybersecurity

Germany is adopting a holistic approach to cybersecurity. Although the BMI leads from a policy-development perspective, operational responsibility is delegated to a dedicated set of agencies and offices from the intelligence community, law enforcement and public-private liaison. Bringing these bodies under the aegis of the BMI is intended to address issues of fragmentation by centralizing oversight and overall responsibility.

2.2. Cyberdefense

Germany defines cyberspace as the "cyber and information space". While this definition is broad and potentially vague, it allows Germany to develop responses to a variety of current international cyber-threats. These include "traditional" cyberthreats such as damage or destruction to critical physical and information infrastructures, but also hybrid warfare, advanced persistent threats, state and non-state cyber-terrorism and media and popular online manipulation. Germany's cyberdefense posture also involves the development of offensive cyber capabilities as well as publically stating the readiness to deploy these capabilities should the need arise.

3. Key national frameworks

3.1. Cybersecurity

Both cybersecurity and cyberdefense are divided into policy-development and oversight responsibilities and the operationalization of that policy. Policy development in cybersecurity is divided between the BMI, the Chancellor's Office and the Federal Foreign Office. Within the BMI in particular, specific operational tasks are delegated to agencies with particular areas of expertise, such as the Federal Office for Information Security (BSI) and the Federal Intelligence Service (BSI). Overall leadership in cybersecurity, however, stems from the Ministry of the Interior.

3.2. Cyberdefense

The Federal Ministry of Defense (BMVg) is responsible for Germany's cyberdefense and, sitting alongside the Foreign Office, Chancellor's Office and BMI, is one of the "big four" ministries contributing to overall oversight and policy development. From an operational perspective the BMVg has a similar structure to the BMI in that specific agencies and bureau are delegated specific tasks relating to areas of expertise. Together, all of the agencies are tasked not only with defending and ensuring the functioning of government and national digital systems and infrastructures, but protecting these from foreign attack and interference. The structure allows for close collaboration with non-military agencies in order to share information and resources in the event of a cyber-attack.

Germany is also in the process of building up an effective cyber command within the army with offensive and defensive capabilities, a cyber-reserve and a cyber-research center.

4. Level of partnership and resources

Germany co-operates with core allies such as NATO and the EU in order to increase cybersecurity internationally. It is actively engaged in developing EU cybersecurity through promoting core legislation and cooperation mechanisms as well as advocating for the development of security standards and rules for vital sectors and key digital service providers.

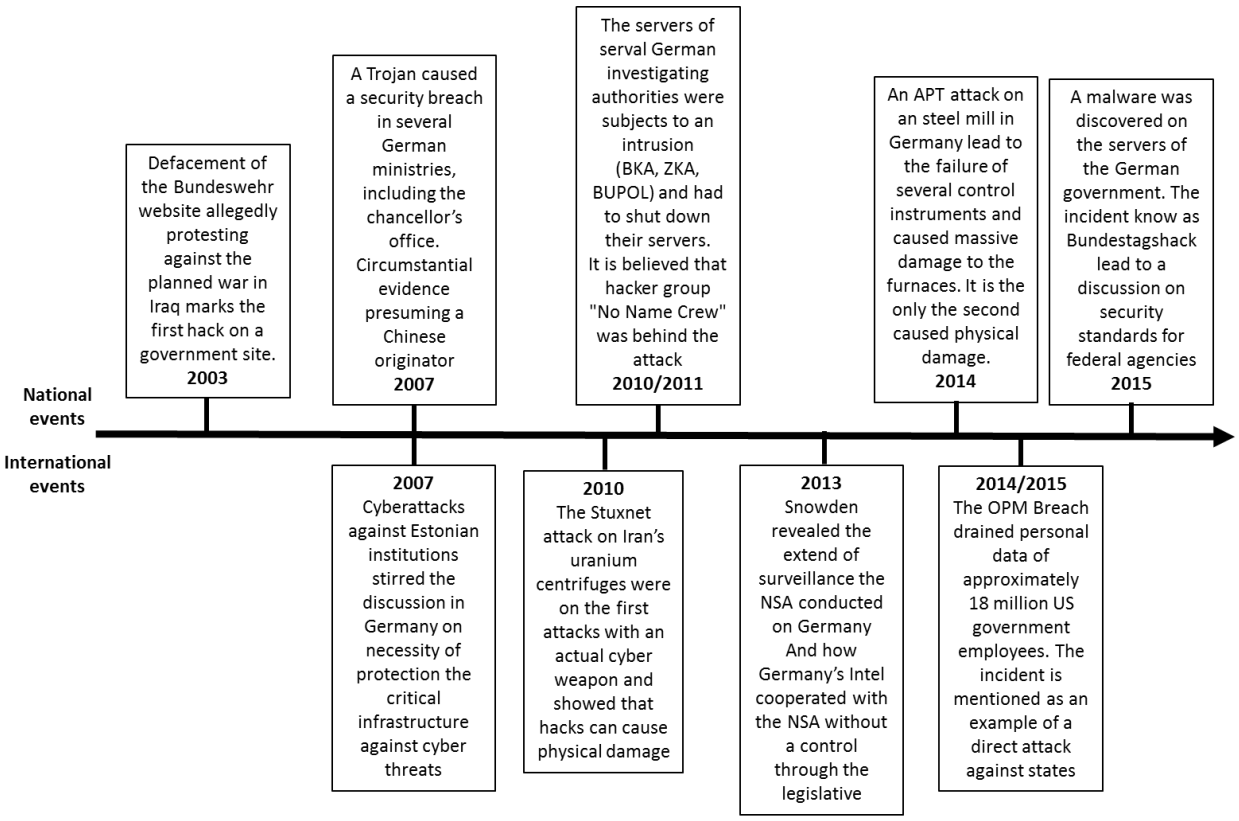
In cyberdefense Germany is an active member of the NATO Cooperative Cyberdefense Center of Excellence in Tallinn.

1. Evolution of national cybersecurity policy (since mid-1990s)

1.1. Threat perceptions: trigger events

Several incidents can be identified that had an impact on the evolution of the German cybersecurity. This is a selection of events that have been explicitly mentioned in the documents or that can be linked to the formulation of a new policy:

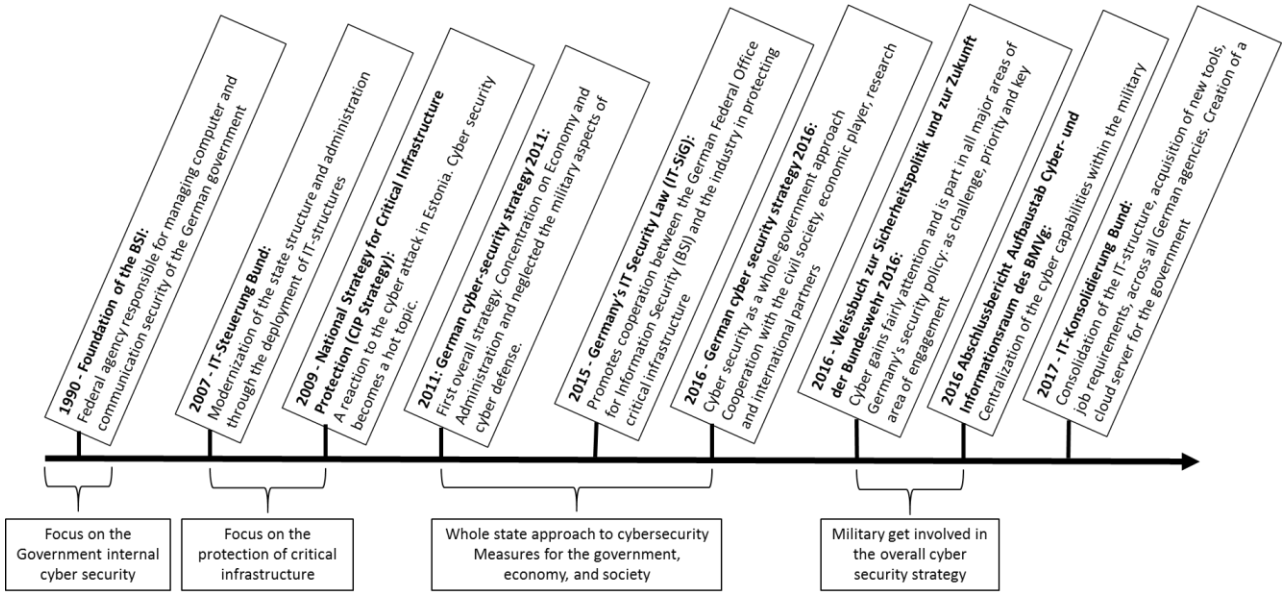
Diagram DE1: Timeline of Trigger Events



1.2. Main policy documents: key shifts in strategy

This section presents the key the shifts in the German cybersecurity and defense strategy partially caused by the events described in the last section:

Diagram DE2: Timeline of Policy developments and Trends



1.3. Organizational structure: key parameters

Germany has a holistic approach to cybersecurity, focusing on the opportunities afforded by digitalization but also acknowledging the threats posed by increased connectivity. Despite this holistic approach, prior to 2016 Germany's cybersecurity policy structure was decentralized with cybersecurity and cyberdefense-related tasks assigned to separate pre-existing agencies, without any new bodies being set up. Germany's new Cybersecurity Strategy of 2016 marks a shift towards a more interlinked and centralized structure.

At the ministerial level, responsibilities are divided between foreign policy, civilian tasks and military tasks. The Chancellor's Office[38] (BKAmt) coordinates the international aspects of cybersecurity policy through the Foreign Office and information-gathering through the Federal Intelligence Service (BND).

The Federal Ministry of Interior (BMI) supervises the civilian and national security aspects of cybersecurity. It is also responsible for the formulation of overall cybersecurity strategy. The BMI highlights that a holistic approach is necessary to protect the state, the economy and the citizens from the increasing exposure to cyberthreats. Hence, it promotes a cybersecurity strategy which involves private actors, Germany's federal states and international partners. Within the BMI, cybersecurity related competences have been delegated to specific offices such as the Cyberdefense Response Center (Cyber-AZ; see page 9).

At the military level, the Federal Ministry of Defense (BMVg) is responsible for the coordination of cyberdefense. With the formation of the Cyber and Information Domain Command (KdoCIR) in 2017, the military aspects of cybersecurity drawn together and centralized. The KdoCIR is equipped with defensive and offensive cyber capabilities.

1.4. Context/Analysis: key national trends

Germany is the fourth largest economy in the world and the largest economy in Europe (Worldbank, 2017). Consequently it is one of the leading nations of the European Union (EU). This role as a global player has only been partially embraced by the German government, however. As a result of its history, Germany still limits the use of its military and curtails its aspirations to become an active global power. A further consequence of this reticence is that Germany's involvement in world politics has been mainly diplomatic and economic.

In recent years, however, Germany has begun to participate in international military operations, particularly as a result of its membership of NATO. It has participated in several NATO missions, such as the peacekeeping operations in Bosnia and Herzegovina in 1995, the deployment of troops in Afghanistan in 2003, patrolling the Aegean Sea in 2016,

[38] See Annex 3 for a list of acronyms, their full German names and their English equivalents.

and in 2017 it deployed troops in Lithuania under the operation “Enhanced Forward Presence”. These operations bring Germany more into the spotlight of world politics and can make them also a target for potential opponents in both the cyber and physical realms.

Due to this shift in its willingness to project a certain amount of hard power, Germany has the ninth highest military expenditure in the world with US$41.1 billion. However, at 1.22% of national GDP German military expenditure is well below the 2% spending goal stipulated by NATO (NATO, 2014). While there have been increased in military spending since 2016 after years of cutbacks (Die Bundesregierung, 2016b), the resources are still limited. As a consequence, Germany’s overall military approach is defensive. The focus lies on protection through resilience and robustness combined with efforts in crisis recognition, prevention and containment.

In parallel to this hard power posture (albeit a defensive one) Germany sees itself as a stable and reliable partner and uses its dominant position in international organizations such as the EU, the UN and OSCE to promote its world view. While its political focus is restricted to domestic issues and the EU, the German government acknowledges that its domestic security policy can be influential for other, external states (Die Bundesregierung, 2016a, p. 22).

This approach has spilled over into Germany’s cybersecurity and cyberdefense policy development. That development prioritizes the unhindered use of information and communication channels as well as the security of resources and energy supply. Since the 1990s, the German government has introduced several projects to increase the security of these communications channels and infrastructures. An all-of-government approach is promoted, one including at the on international, national and federal state level as well as close cooperation between the government, the army, and private actors to ensure functioning and resilient information and communications systems.

The plurality of approaches in combination with the federal structure of the government has led to parallel structures being developed with duplication or incompatibility of systems. In the most recent policy papers, there is therefore a trend towards restructuring and reorganizing the existing projects on IT security and attempting to coordinate new measures more centrally in order to increase efficiency and harmonization.

2. Current Cybersecurity Policy

2.1. Overview of key policy documents

2.1.1. White Paper on German Security Policy and the Future of the Bundeswehr 2016

The most recent document which sets out German national security policy is the White Paper on German Security Policy and the Future of the Bundeswehr 2016. This White Paper lists a number of cyber and information domain risks directly below transnational terrorism as one of the main threats to German security (Die Bundesregierung, 2016a). This is a marked contrast to the previous White Paper of 2006 which only mentioned cyberspace once as a potential target for and source of criminal activities, terrorism, and military attacks (BMVg, 2006). Cybersecurity issues have therefore gone up the prioritization ladder in the ten years to 2016, to the extent that they are considered a major threat to national security. Reflecting this reprioritization, the 2016 White Paper makes mention of the various threats emanating from cyberspace, ranging from attacks on critical infrastructure through to information warfare, and makes explicit the need to increase international cooperation against cyberthreats.

In terms of national preparedness and capabilities, the 2016 White Paper states it is necessary for Germany to build up and enhance both defensive and offensive capabilities against complex cyber-attacks. However, the White Paper does not elaborate what those capabilities are, a common trait in a number of national cybersecurity, cyberdefense or national security policies. In addition, the White Paper highlights the need to modernize the military and make key technologies more resilient. This indicates that current military systems are considered, at least to some extent, outdated. Furthermore, the document states the need to consolidate the fragmented responsibilities and structures in order to enhance the IT capabilities and the digitalization of the military (Die Bundesregierung, 2016a, p. 93).

2.1.2. Cybersecurity Strategy for Germany 2016

The Cybersecurity Strategy for Germany (CSD) of 2016 is the overall national strategy intended to make Germany more resilient against cyber risks. The CSD of 2016 replaces the previous document of 2011. The earlier document contained 10 measures to promote cybersecurity in Germany, measures which focuses mainly on civilian measures and mentions the military only on the sideline (BMI, 2011, p. 5). The majority of those measures were not concrete actions but rather statements to increase the cybersecurity through closer cooperation within the state, with economic actors and with international partners. That being the case, the 2011 strategy initiated two important national agencies, National Cyberdefense Center (Cyber-AZ) and the National Cybersecurity Council (NCSR).

The current strategy of 2016 builds on its predecessor by stating 29 goals that are linked to more concrete measures and includes more attention paid to the role of the military within the whole German cybersecurity structure (BMI, 2016). These measures will be addressed in more detail in Section 2.2 below.

2.1.3. Final Report of the Commission of the Ministry of Defense on the Cyber- and Information Space 2016

The Final Report of the Commission of the Federal Ministry of Defense on the Cyber- and Information Space (AACI)[39] focuses on civilian and military defense aspects of the cybersecurity. There are no previous version of such a report. The report recommends establishing one center for the civilian aspects of defense and one for the military. The report elaborates in detail how the restructuring should be executed and provides a timeline on the required steps towards a more centralized and efficient cyberdefense (BMVg, 2016).

2.1.4. Concept on personnel support for the cyber-community of the Bundeswehr (Cyber-Reserve) 2017

Due to the restructuring of Germany's cyberdefense framework, there is need for additional IT specialists. To overcome the current dearth of expertise, in 2017 the BMVg posited the establishment of a "cyber-reserve". This reserve would be made up of experts from different aspects and fields of IT and cybersecurity. The idea of such a cyber-reserve was already mentioned in the Report on the Cyber and Information Space from 2016 but the 2017 concept document formalized the proposal.

[39] Abschlussbericht Aufbaustab Cyber- und Informationsraum des BMVg

2.2. National cybersecurity strategy: fields, tasks, priorities

The CSD of 2016 is an inclusive and comprehensive strategy intended to increase cybersecurity through the implementation of 29 specific measures, measures grouped into four fields of action:

1. Promoting secure and autonomous action in the digital environment.
2. Increasing cooperation in cybersecurity between the state and economical partners.
3. Building a sustainable and capable overarching cybersecurity structure.
4. Increase the participation of Germany in building a European and international cybersecurity strategy.

The CSD argues that cybersecurity requires, first and foremost, risk-adapted behavior and secure systems. Basic measures such as regular workshops and certifications for IT products and companies could prevent a large number of cyberattacks by improving education, awareness and the resilience of digital systems.

As is clear from the four fields of action Germany's current cybersecurity strategy is geared towards socio-economic goals. The German government regards the creation of an innovation-friendly and creative environment for IT research and technology companies as a key pillar of successful cybersecurity. At the same time protecting citizens and companies in Germany against threats from cyberspace is also seen as a core task of the state.

To achieve these goals and reduce fragmentation of responsibility as well as to increase efficiency and harmonization, the strategy promotes centralization and closer cooperation in the civilian aspects part of the cybersecurity. This is to be achieved through the creation of a coordination office. The Central Office for IT in the Security Sector[40] (ZITiS) was established and tasked with identifying synergies in the still-decentralized cybersecurity architecture.

Additionally, the strategy underlines the fact that closer cooperation with European and international partners is necessary to make Germany more secure, since cyberspace is not constrained by national borders, a single or even regional legal jurisdiction or assigned areas of government agencies' responsibilities (BMI, 2016).

2.3. National cyberdefense strategy: fields, tasks, priorities

Although it is not a formal, specific and separate cyberdefense strategy document, the Final Report of the Commission of the Federal Ministry of Defense on the Cyber- and Information Space (AACI) of 2016 contains what can reasonably be described as Germany's current cyberdefense strategy. It sets out two organizational measures or goals:

- The formation of the Section for Cyber and IT (CIT) within the Federal Ministry of Defense (BMVg)
- The formation of a military unit focusing on the cyber and information space to be called the Cyber and Information Domain Command (KdoCIR)

The AACI therefore divides German national cyberdefense is divided into two parts, each part headed by one of these two agencies. The AACI explains in detail how these two units are built and which units are affected from this restructuring. On the one hand the CIT is intended to bundle together all non-military tasks related to the usage and protection of the IT infrastructure of the BMVg. This is not a defense task *per se* but instead ensures that the civilian bureaucracy and IT systems are protected and defended. Military operations and actions run parallel to this and form the second part of German cyberdefense. All military units operating in the cyber and information space come under the command of the KdoCIR. The KdoCIR is also intended to act autonomously from the other military branches to defend the cyber and information realm.

The statement in the AACI that cyberdefense always contains defensive and offensive capabilities (BMVg, 2016, p. 5) implies that the KdoCIR will also be able to conduct offensive operations. However, the term "cyber and information space" is a broad definition of the cyber realm. This means that the AACI refers not only to threats against the Bundeswehr or the government but also against society, the democratic system and the German economy. In this vein, the AACI makes specific mention of the dangers presented by hybrid warfare, advanced persistent threats, and attacks against the critical infrastructure such as the Stuxnet attack, the OPM-Breach and the Bundestagshack. In this multi-target and multi-threat environment, the KdoCIR is expected to react mainly to high-end threats.

2.4. Context/analysis: key policy principles

Germany's cybersecurity policy is led by the Ministry of Interior (BMI) and promotes a comprehensive approach to cybersecurity stretching from economic and civilian partners to the military. Operating and working alongside civilian

[40] Zentralen Stelle für Informationstechnik im Sicherheitsbereich

cybersecurity organs, the BND and military are envisaged as important pillars of this new broader conceptualization of cybersecurity. The BND is tasked with building an early warning system to detect cyberthreats and the military is established as the key actor in cyberdefense.

The overarching cybersecurity strategy is presented in the in the Cybersecurity strategy for Germany 2016 and focuses on measures to increase cybersecurity by building up defensive capabilities by building up a comprehensive cybersecurity architecture within the government and increase the cooperation with international, economic partner and the military. Sitting alongside the CSD, the AACI of 2016 clarifies the military aspects of the cybersecurity architecture and recommends centralizing the cyberdefense tasks in the BMVg and the Bundeswehr. In one important respect, the AACI creates policy parity with states such as the UK, France and the US report. It argues that the cyber and information realm is own dimension alongside land, air, sea, and space, a dimension in which state power and capabilities can be expressed and deployed. The concept document on personnel support for the cyber-community of the Bundeswehr the problem of missing IT-specialists in the BMVg necessary for a capable cyberdefense.

All the current policy documents published between 2016 and 2017 are highly interconnected and make reference to each other, either as direct references or by maintaining a standard, harmonized approach. The inclusion of the military in the current cybersecurity strategy marks a shift from the previous grand strategy of 2011 and indicates a change in the perception of threats derived from cyberspace: criminal activity is acknowledged but is described as a lesser threat to national security and citizen safety than foreign state action or cyberterrorism.

Despite this change in priorities, the larger German strategy focuses to a large extent on cooperating with economic actors in order to secure cyberspace. This is due in part to the government lacking certain necessary technical capabilities and expertise, but also to historic reticence to engage in solo military operations.

The current documents also indicate that the middle to long-term goals for German policy in this sector is to further draw together and centralize capabilities within the civilian part of the government and the military alike. The centralization of cyber tasks in the military, through the formation of the ZITiS as a cooperation and coordination platform and the concept for recruiting IT-specialists, are concrete steps into this direction.

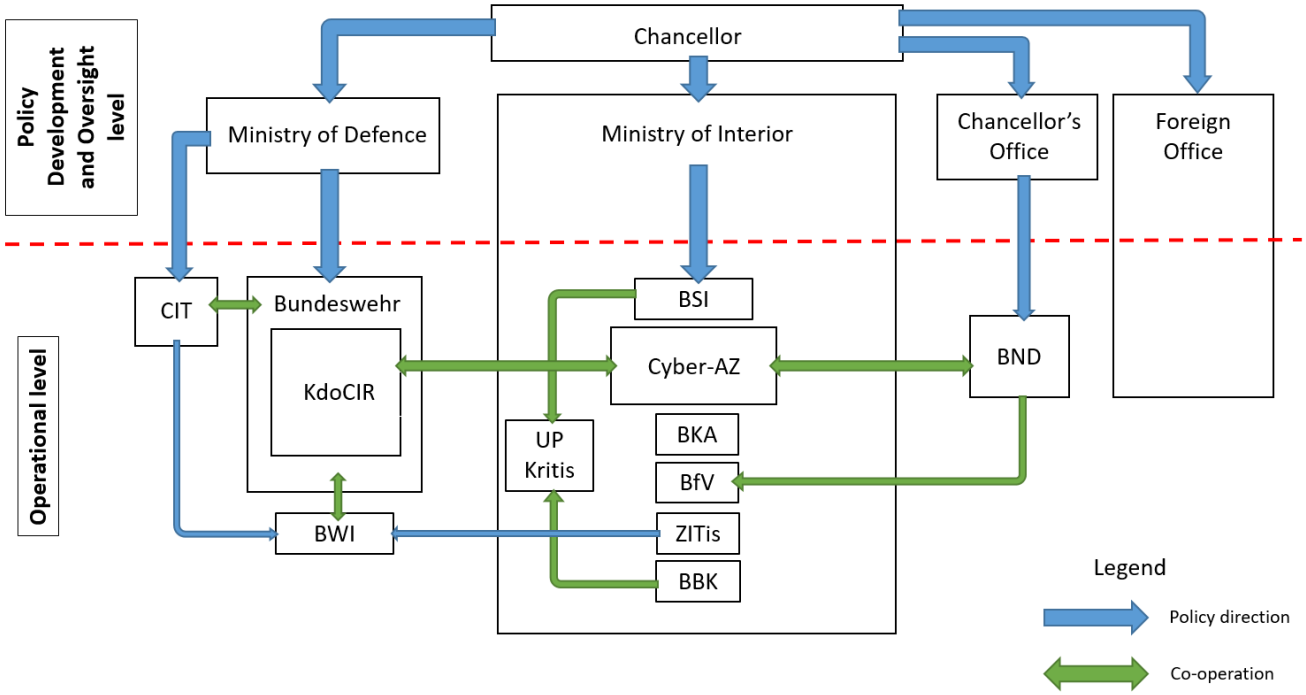
There is one element of German policy which merits particular attention. Because of the clear defensive posture set out in the policy documents examined, as well as an historic reticence to be seen to be projecting any form of hard power, it is surprising that Germany states in the AACI that it will undertake offensive operations in cyberspace should there be a need to do so. On the face of things, this acknowledgment shifts German policy as a whole away from civilian posture and more towards the military. The reality is, however, that the clear leadership role of the BMI and subordinate role of the Bundeswehr and Ministry of Defense to that leadership show that, on a spectrum of civilian vs military policy development, cybersecurity and cyberdefense remain civilian-led policy areas.

3. Current public cybersecurity structures and initiatives

3.1. Overview of national organization framework

Diagram DE3 below provides a graphical representation of the organization of Germany's cybersecurity apparatus.

Diagram DE3: Oversight Organigram



3.2. National cybersecurity structures and initiatives: organization, mandate, legal aspects, operational capabilities

3.2.1. Federal Ministry of Interior

As with a number of other national frameworks in this policy sector, German cybersecurity and cyberdefense policy is divided into a policy development and oversight section and an operational section. Overall strategic leadership in cybersecurity comes from the **Federal Ministry of the Interior (BMI)**. The ministry's main responsibility is the formulation and ongoing development of national cybersecurity strategies aimed at the reduction of cyber risks to an acceptable level. The BMI publishes all relevant governmental policy documents on cybersecurity and is responsible for inter-governmental coordination between the principle federal government measures regarding critical infrastructure (BMI, 2009).

In terms of operationalizing core aspects of cybersecurity such as IT-security, emergency preparedness and response, the BMI receives administrative assistance from several subordinate agencies.

3.2.1.1. Federal Office for Information Security

The **Federal Office for Information Security (BSI)** is located within the BMI and is the federal authority responsible for information security on a national level (§ 1 BSIG). Specifically, the BSI is responsible for the protection of government IT systems, the examination of IT-security risks, evaluating and certifying of IT-systems and setting IT security standards. With the revision of the Act for the Improvement of Information Technology System Security (BSIG) in 2017, the tasks of the BSI have been expanded to include oversight of critical infrastructures (BMJV, 2017). The operators of critical infrastructure are now required to demonstrate to the BSI their compliance with current IT-security standards. With the consent of federal regulators the BSI is entitled to ask for any identified defects to be corrected and remedied (§ 8a BSIG). Furthermore, the BSI is currently establishing "Mobile Incident Response Teams" (MIRTs) that provide technical support for community-critical institutions (e.g. critical infrastructure) in the case of a cyber-attack (BMI, 2016).

3.2.1.2. Federal Office for the Protection of the Constitution

The **Federal Office for the Protection of the Constitution (BfV)** is also located within the aegis of the BMI. It is Germany's primary counter-intelligence agency. It is tasked with handling all espionage activities involving foreign intelligence activities in or against Germany. The BfV also gathers information on cyberespionage and cyberattacks with extremist connotations. In addition to the MIRTs of the BSI, the BfV is currently building up "Mobile Cyber-Teams" that can be deployed in the case of cyber-attacks which may originate from foreign intelligence services or terrorist organizations.

3.2.1.3. Federal Criminal Police Office

The **Federal Criminal Police Office (BKA)**, also located at the BMI, focuses specifically on cybercrime. In addition to the mobile teams in the BfV and the BSI, the BKA is currently developing Quick Reaction, which will have the capabilities for conducting initial criminal procedural measures on-site after a cyber-incident in order to secure evidence for a prosecution (BMI, 2016).

3.2.1.4. Federal Office for Civil Protection and Disaster Response

The **Federal Office for Civil Protection and Disaster Response (BBK)** is responsible *inter alia* for the protection of critical infrastructure. In 2007, the BBK, the BSI and the operators of critical infrastructure established the public private partnership UP KRITIS. Since 2013, cybersecurity has been a key element of the UP KRITIS which serves as an exchange platform between the operators of critical infrastructure and the government. It is an instrument designed to ensure a high level of cybersecurity for its participants (UP KRITIS, 2013).

3.2.1.5. Cyberdefense Response Center

The **Cyberdefense Response Center (Cyber-AZ)** is subordinate to the Federal Office for Information Security (BSI) within the BMI. As part of its remit it collaborates with the Federal Office for Civil Protection and Disaster Response (BBK) and the Federal Office for the Protection of the Constitution (BfV). In addition, the Cyber-AZ provides operational support to the Federal Criminal Police Office (BKA), Federal Police Office (BUPOL), Customs Investigation Bureau, Federal Intelligence Service (BND) and the military. Due to this extensive collaborative network the Cyber-AZ is an important hub for the exchange of information, operational expertise and best practice.

The Cyber-AZ has its own analytical capabilities and creates its own cyber situation picture. The main tasks of the Cyber-AZ are:

- The assessment of cyber-attacks
- The inter-governmental coordination of responses
- The provision of ICTS.
- Providing information on systemic weaknesses and vulnerabilities
- Analyzing channels of attacks, and compiling profiles of perpetrators.
- Providing recommendations to the National Cybersecurity Council

Furthermore, in the event of a critical national cyber incident, the Cyber-AZ becomes a cyber-incident response center, from where all defense measures are coordinated. In order to improve the necessary operational cooperation in general, but also specifically in the event of national crises, exercises and training with all involved governmental entities are organized by the Cyber-AZ (BMI, 2016).

3.2.1.6. The Central Office for Security in Information Technology (ZITiS)

The **Central Office for Security in Information Technology (ZITiS)** holds no operational powers but develops customized methodologies, products and overarching strategies regarding operational implementation. ZITiS is responsible for the IT-governance, IT-services, information security of all ministries and the oversight of the recently nationalized BWI.

3.2.2. Federal Chancellor's Office

Sitting alongside the BMI are two other federal departments dealing with cybersecurity. The **Chancellor's Office (BKAmt)** is one such department and is an important hub for cybersecurity in Germany. Located within the Chancellor's

Office is the **Federal Intelligence Service (BND)**. This the Office in general assists with policy development, from an operational perspective the BND collects information on cyberespionage and cyber-attacks targeting governmental institutions and/or critical infrastructure.

Within its legal framework, the BND is entitled to observe attacks as they are occurring in real time and to register the unauthorized flow of information. Additionally, the BND provides other government entities with "signals intelligence support to cyberdefense" and manages an own current picture on the threat situation (BMI, 2016).

3.2.3. Federal Foreign Office

The **Federal Foreign Office** is responsible for all foreign policy aspects of Germany's cybersecurity policy. It represents Germany in international organizations such as the UN, the OSCE, the Council of Europe, the OECD, and in NATO. Germany argues that effective cybersecurity requires international cooperation and trust. As a result, the Foreign Office pushes for the development and implementation of trust building-measures such the acceptance of the international laws, an agreement on norms, and for states to engage in responsible behavior in cyberspace (Auswärtiges Amt, 2017).

Due to the combination of its policy development capacities as well as its remit for directly engaging in trust-building and international aspects of cybersecurity, the Foreign Office can be said to sit astride the policy-operational divide. This is a unique position in the German framework. While the BMI also engages in both policy development and operationalization, it does so by assigning specific operational tasks to specific agencies an offices. Such a detailed divide and delegation is not made clear for the Foreign Office.

3.2.4. Ancillary agencies

In addition to dedicated cybersecurity agencies and bodies, there are several other federal government entities which play a prominent role in German cybersecurity. Those with the most relevance to this present analysis are:

- The **National Cybersecurity Council Association** (Cyber-SR). This body includes the federal states, representatives of large and middle-sized companies, operators of critical infrastructure and high-level representatives of federal agencies. The goal of the Cyber-SR is to bring together knowledge from economic entities and the government and identify relevant trends and areas that require improvement. The Cyber-SR supports the BSI in the formulation of the national cybersecurity strategy and consulates the federal government regarding cyber-security (BMI, 2016).
- The **Federal Government Commissioner for Information Technology (BfIT)** is tasked with expanding the current intra-governmental IT-coordination into an IT-management structure.
- The **IT-Council** brings together representatives from all government ministries including those responsible for IT at the Chancellor's Office as well as the Federal Commissars for Media and Culture (BKM) and Press and Information Office (BPA). The Council formulates overarching IT-strategies, IT-architecture and IT-standards as well as overseeing the governance of overarching projects concerning IT-consolidation. The IT-Council meets twice a year.
- The **IT-Management Group** oversees the government's overall IT framework. It oversees the IT-Council, sets out the IT-framework concept, mediates the actions of governmental entities when these run counter to its decisions and or the resolutions of the IT-council, and proposes resolutions for contested matters in the IT-council.
- The **IT Officer Conference** prepares the resolutions of the IT-Council and is responsible for their implementation. It decides on operational IT matters based on the resolutions of the IT-Council.

3.3. National cyberdefense structures and initiatives: organization, mandate, legal aspects, operational capabilities

The **Federal Ministry of Defense (BMVg)** is responsible for German cyberdefense, policy development and oversight of the military against cyberthreats. It sits alongside the Chancellor's Office, the BMI and the Foreign Office at the level of policy development and, like the BMI, has delegated core operational tasks to key agencies and bodies. With the revision of the cyberdefense structure mentioned in the 2016 Report on Cyber and Information Space, two new entities have been created: the Section for Cyber and IT and the Cyber and Information Domain Command.

3.3.1. Abteilung Cyber/IT (CIT)

The **Section for Cyber and IT (CIT)** is responsible for the acquisition, use, and protection of the IT structure of the BMVg, the nationalized company BWI (cf. section 4.1), and the Bundeswehr. The CIT draws together the fragmented responsibilities for the smooth running of the separate units of the BMVg into one organizational structure. The idea is that the CIT increases the development and deployment of new technologies and harmonizes the current soft- and hardware capabilities in order to increase the capability of the whole BMVg.

3.3.2. Cyber and Information Domain Command (KdoCIR)

The **Cyber and Information Domain Command (KdoCIR)** is not considered a traditional military branch, such as the army, air force, or navy. Instead, the KdoCIR is intended to have the capability to act independent of the other branches. The primary tasks of the KdoCIR are:

- Contributing to the protection of national critical infrastructure.
- Conducting computer network operations (CNO) and electronic warfare tasks.
- Recognizing propaganda and disinformation in crisis areas.
- Participating in opinion-making in areas of interest to the Bundeswehr.
- Compiling a comprehensive military intelligence situation picture and an overarching cyber situation picture (BMVg 2016).

In order to fulfill these tasks, the KdoCIR oversees 25 existing offices related to cyber in Germany and the German unit of NATO's CCDCOE in Tallinn (Bundestag, 2017). This involves 13,700 individual posts. It is anticipated that the total number of IT-relevant posts will increase to 20,000 by 2021 but without any major changes to the existing geographic locations (BMVg, 2016, p. 22).

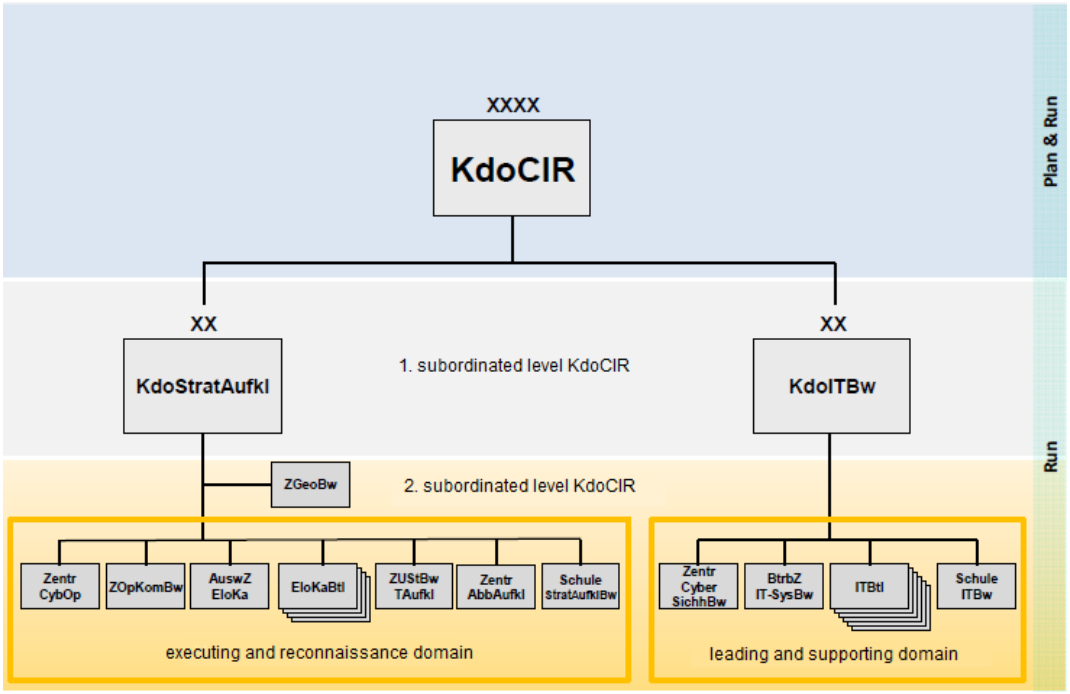
To achieve its goals, the KdoCIR includes a number of distinct entities. There are:

- The **Strategic Reconnaissance Command (KdoStratAufkl)** and **IT Command of the Bundeswehr (KdoITBw)**. These bodies comprise the two main pillars of the KdoCIR. The Strategic Reconnaissance Command focusses on intelligence information management and reconnaissance in cyberspace. Its main tasks are the issuing and provision of an intelligence situation picture concentrating on the tactical and operational level. These tasks cover current risks and hybrid threats. Previous responsibilities of the KdoStratAufkl included the development of joint armed forces intelligence training and the coordination of joint armed forces intelligence capabilities which provided information to the planning staff of the KdoCIR (BMVg 2016).
- The **Geoinformation Center of the Bundeswehr (ZGeoBw)** is assigned to the Strategic Reconnaissance Command (BMVg, 2016). Its areas of operation are geo-information systems, big data analysis, situation-related consultation in applied geography and alternative technologies for navigation, positioning and time determination (BMVg, 2016). Working with the Geoinformation Center is a joint situation fusion center and a military intelligence situation center.

  At the joint situation fusion center a "consolidated situation picture" is issued. This combines separate situation pictures from military intelligence, the information environment, the civilian environment, the IED-situation, IT-system operations of the Bundeswehr and the cybersecurity situation picture. The military intelligence situation center provides a comprehensive intelligence picture contributing to all phases of military operation and crisis provision (BMVg 2016).
- The **IT Command of the Bundeswehr (KdoITBw)** has several important remits. It is in charge of the conduct of disciplinarily assigned IT-units which operate the IT-systems of the Bundeswehr (BMVg, 2016a). Furthermore, this Command is responsible for the **Center for Cybersecurity of the Bundeswehr (ZCSBw)**, consisting of the former IT-Center of the Bundeswehr (IT-ZentrumBw) and the IT-Training Academy of the Bundeswehr. The IT Command also responsible for the IT evaluation, including prototyping and coding. Finally, it provides guidance to IT-project managers and in all business related matters regarding the integration of IT-services in the IT-systems of the Bundeswehr (BMVg, 2016, p. 26).

The interrelationships of the various agencies of the Cyber and Information Domain Command are summarized in Diagram 4 below.

Diagram DE4: the Cyber and Information Domain Command



3.3.3. Cyberdefense Reserve

The German government sees cybersecurity as a "whole-of-state" issue, where the participation of economic, social and academic entities is essential. In order to capitalize on the existing knowledge and competences outside of the active military forces, the Ministry of Defense (BMVG) propose the establishment of "cyber-reserve", similar to that of other countries such as France (BMVg, 2016, p. 5). The proposal presents three main aims of such a reserve:

1. The creation of additional forces that can temporarily support the Cyber and Information Domain Command in the case of large-scale cyber-attacks.
2. The building up of strong cyber units consisting of IT experts of different fields through mutual exercises inside and outside of Germany.
3. Increasing cooperation and dialogue between IT experts in the economy and the military.

The proposal recommends recruiting managers, scientists and top officials from other agencies for specific projects, in a similar manner to external consultants. Furthermore, the proposal states that current armed forces personnel and those in the process of leaving who have fundamental IT knowledge should be informed of the possibility of joining the cyber reserve and actively be courted. The proposal also considers the possibility of attracting soldiers without the necessary IT education, but with necessary informal knowledge. In addition, it recommends considering potential candidates that do not meet the normal requirements for the military, such as physical fitness or status of nationality, but who have relevant or beneficial IT knowledge and experience.

To attract candidates for the reserve beyond informing active service personnel of its existence, the proposal recommends getting in touch with other agencies, the administration and IT hardware and software companies in order to identify potential synergies a cyber-reserve could develop. That being said, in the future, members of this cyber-reserve would be drawn primarily from the study programs of the University of the Bundeswehr in Munich.

Finally, the proposal also makes it clear that it is necessary for the Bundeswehr to become a more attractive employer for such specialists in comparison to private corporations. However, the report misses out on elaborating how the Bundeswehr could create incentives for the potential candidates to join the cyber-reserve.

3.4. Context: key public organizational framework

The current revision process of Germany's cybersecurity and cyberdefense structure aims to clarify responsibilities, increase cooperation between different entities and create contact points for domestic and foreign agencies alike. The restructuring of Germany's cybersecurity architecture mainly uses capabilities and resources already in place but tries

to align them in order to make them more efficient. The Chancellor's Office operates as a hub for this centralization and harmonization but overall leadership comes from the Ministry of the Interior (BMI).

Within the BMI, the main shift in structure has been the formation of Central Office for Security in Information Technology (ZITiS), which is designed to support other agencies with its technical expertise. The newly created mobile incident teams under the control of the Federal Office of Information Security (BSI) and the mechanisms for upgrading the Cyber-AZ to a national crisis center in the event of a serious nation-wide cyber-incident indicates that the German government wants to reduce the reaction time for smaller and larger cyber-related incidents alike. The new functions of the Cyber-AZ also show the government recognizes the potential for Germany being the target of larger (military) cyber-attacks.

The most significant changes of the restructuring within the cybersecurity architecture can be found in the Ministry of Defense (BMVg), where both non-military and military cyber capabilities have each been centralized. The Cyber and Information Domain Command (KdoCIR) provides the government with an effective instrument against cyber-incidents with its offensive and defensive capabilities. The open statement on the usage and capability of offensive capacities could be interpreted as acting as a deterrent against the actions of potential aggressors. The decision to give the Cyber and Information Domain Command the responsibility of identifying disinformation campaigns and propaganda is a surprising move from the German government, since the military is not normally involved in verifying non-military information. While it is unclear at this stage how far these competences will go, it highlights the relevance of the topic for the government. Given the still-strict parameters for German military operations, its cyberdefense capabilities still have a defensive posture, one highlighted by the deterrent effect of its offensive capabilities.

Overall, the formation of the Cyber and information Domain Command itself demonstrates the aspiration and willingness of Germany to be a part of the highest levels of international cybersecurity and cyberdefense operation and involvement and shows a more active positioning regarding securing cyberspace within alliances such as NATO. Nevertheless, were German policy to be placed on a spectrum of civilian vs military or defense posture, the leadership structure instituted shows Germany favors a civilian rather than military leadership.

4. Current cyberdefense partnership structures and initiatives

4.1. Public-Private cyberdefense partnerships:

Between 2006 and 2016 the Bundeswehr Informationstechnik GmbH (BWI) was a public-private partnership (PPP) which included the Bundeswehr, Siemens and IBM. The goal of this partnership was to modernize the nonmilitary ICT of the Bundeswehr. The German government ended the cooperation with Siemens and IBM in December 2016 and the BWI is now completely controlled by the Bundeswehr. One reason for this move was the desire to use the knowledge acquired to develop the German military's IT-infrastructure. In the long term, the plan is to make the BWI the main equipment and systems retailer for the whole government (BWI 2017).

4.2. International cyberdefense partnerships:

The focus of Germany's international cooperation priorities are the EU and NATO. Germany has sought to increase cybersecurity standards on a European level through the European Union. In 2016, the European Parliament adopted the first EU legislation on cybersecurity - the Directive on Security of Network and Information Systems (NIS Directive). The NIS Directive established a network for cooperation and coordination against cyber incidents, requires EU Member States to be properly equipped for cyber incidents, and sets security standards and rules for vital sectors and key digital service providers (European Commission, 2016). Additionally, the EU plans to build a European Cybersecurity Coordination Platform with a "coordinator" leading the platform with competences similar to the European Counterterrorism Coordinator (European Commission, 2017).

Germany's preferred method of problem resolution is through multilateral means and cyberdefense is no expectation. Germany has a specialist unit stationed at NATO's Cooperative Cyberdefense Center of Excellence (CCDCOE) in Tallinn, Estonia and it can be assumed that cooperation on a military level will be further intensify with the new Cyber and Information Domain Command.

4.3. Cyberdefense awareness programs:

Germany promotes cybersecurity through the BSI and the IT-Grundschutz program (BSI, 2017). However, there is no specific program for promoting awareness for cyberdefense.

4.4. Cyberdefense research programs:

In 2013, the University of the Bundeswehr in Munich founded the Forschungszentrum Cyberdefense (CODE). The areas of research are on cybersecurity, smart-grid technology, critical infrastructure, e-health and mobile security (Universität der Bundeswehr, 2013). The research center now hosts 11 professorships. Alongside purely educational and research aspects, the German Ministry of Defense wants to promote the center as a place for cooperation with private actors. One proposal is to build up cyber clusters, where security representatives from national, corporate and civilian actors could communicate with each other and work together on the development of cyberdefense tools (BMVg, 2016, pp. 35–36).

In addition to this cooperation, the University of the Bundeswehr is stimulating the creation of a so-called "cyber innovation hub" at the Munich campus where private sector "spin-offs" working in the field of cyber-defense could settle and benefit from the access to experts and proximity to the Bundeswehr as a potential customer. This innovation hub at the University of the Bundeswehr in Munich has a budget of 25 Mio. Euro listed for the next three years to acquire talents and technological funding (Reinhold, 2017).

Outside of the academic environment, it is anticipated that the newly formed ZITiS will play a vital role in researching and developing methods and tools for all relevant agencies. It is planned that ZITis will support other agencies with their technical knowledge in the fields of digital forensics, surveillance of telecommunication, crypto-analysis, big data analysis, and technical aspects in the field of espionage, defense, and organized crime (BMI, 2017).

4.5. Cyberdefense education and training program

In 2018, the CODE will begin hosting a degree course with 70 graduates annually. The course will educate students on cybersecurity and cyberdefense and are, to a large degree, compiled for future officers of the army (BMVg, 2016, p. 35).

In its publications, the Ministry of Defense also mentions training exercises, staff exchange or rotation between the different agencies and the creation of overarching carrier paths for IT-related positions with comparable and clear job profiles (BMVg, 2016).

5. Annex 1: Policy Spectra

These sliding scales represent three policy spectra:

4. The extent to which policy development and management in cyberdefense and cybersecurity is centralized;
5. The extent to which these areas fall under civilian or military oversight and
6. Whether or not the state under examination has a defensive or offensive cyberdefense posture.

As set out in the introduction to this collection, a state's position on these sliding scales is derived from the analysis in the snapshots. For example, if a state concentrates a significant amount of policy development and implementation responsibility in only a few or a single entity, it is reasonable to conclude that that state operates a more centralized approach to cybersecurity and defense leadership. Similarly, if responsibility in these sectors is placed in the defense ministry then there will be a greater degree of military rather than civilian oversight, and if the possession of offensive cyberdefense capabilities is explicitly stated in the policy literature, a state can reasonably be said to maintain an offensive cyberdefense posture, even if specific capabilities and tools are not mentioned.

5.1. Centralization vs Decentralization of Leadership

Diagram DE6: Spectrum of Centralization vs Decentralization of policy development and management

Centralized control -----X---------- Decentralized control

5.2. Civilian vs defense posture and oversight

Diagram DE7: Spectrum of Civilian-Defense cybersecurity posture and oversight

Civilian oversight ----------X---------- Defense

5.3. Offensive vs defensive capabilities

Diagram DE8: Spectrum of Offensive vs Defensive cyberdefense capabilities

Offensive----------X---------- Defensive

6. Annex 2: Glossary of Terms and Key Definitions

Term	Definition
Civilian cyber security	Civilian cyber security focuses on all IT systems for civilian use in German cyberspace (BMI, 2011, p. 9).
Critical infrastructures	Critical infrastructures are organizations or institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, considerable disturbance of public security or other dramatic consequences. At federal level, the following areas have been identified (BMI, 2011, pp. 9–10): ▪ Energy ▪ Information technology and telecommunication ▪ Transport ▪ Health ▪ Water ▪ Food ▪ Finance and insurance sector ▪ State and administration ▪ Media and culture
Cyberattack	A cyber-attack is an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security. The aims of IT security, confidentiality, integrity and availability may all or individually be compromised.
Cyberdefense	German policy presents three terms that would also be translated to the English “cyber defense”: ▪ “Cyber Defense” comprises the preemptive and reactive measures against cyberattacks targeting processed, saved or transmitted information, the IT system itself or the associated control instruments as well as the tools used for the recovering after an attack (BMVg, 2016). ▪ Cyber-Abwehr is part of the Cyber-Verteidigung. It comprises only defensive measures to protects the operation capability, the protection of the own IT and weapon systems (BMVg 2016). ▪ Cyber-Verteidigung are the existing defensive and offensive capabilities of the Bundeswehr within the constitutional boundaries necessary for the protection against cyberattacks, the protection of the own IT-, information-, and weapons systems. This definition comprises all tasks related to the ensuring of IT-security, cyberdefense, computer network operations, and shielding of the IT (BMVg 2016).
Cyberespionage	Cyber-attacks directed against the confidentiality of an IT system, which are launched or managed by foreign intelligence services.
Cybersabotage	Cyber-attacks against the integrity and availability of IT systems (BMI, 2016, p. 9).
Cybersecurity	(Global) cyber security is the desired objective of the IT security situation, in which the risks of global cyberspace have been reduced to an acceptable minimum. Hence, cyber security in Germany is the desired objective of the IT security situation, in which the risks of the German cyberspace have been reduced to an acceptable minimum. Cyber security (in Germany) is the sum of suitable and appropriate measures.
Cyberspace	Cyberspace is the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace (BMI, 2011, p. 9). For the BMVg, this definition is expanded and also cover IT-systems that contains data ports but are not accessible from the open web and the internet.
Military cyber security	Military cyber security focuses on all IT systems for military use in German cyberspace (BMI, 2011, p. 9).

7. Annex 3: Abbreviations and Acronyms

Abbreviation/Acronym	English	German
AACI	Final Report of the Commission of the Federal Ministry of Defense on the Cyber- and Information Space	Abschlussbericht Aufbaustab Cyber- und Informationsraum des BMVg
BBK	Federal Office of Civil Protection and Disaster Assistance	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BfV	Federal Office for the Protection of the Constitution	Bundesamt für Verfassungsschutz
BKAmt	Chancellor's Office	Bundeskanzleramt
BKM	Federal Commissars for Media and Culture	Staatsministerin für Kultur und Medien
BMI	Federal Ministry of Interior	Bundesministerium des Inneren
BMVg	Federal Ministry of Defence	Bundesministerium der Verteidigung
BND	Federal Intelligence Service	Bundesnachrichtendienst
BPA	Press and Information Office	Bundespresseamt
BSI	Federal Office for Information Security	Bundesamt für Sicherheit in der Informationstechnik
Bw	German armed forces	Bundeswehr
BWI	Bundeswehr Information Technique LLC	Bundeswehr Informationstechnik GmbH
Cyber-AZ	National Cyberdefense Centre	Nationales Cyber-Abwehrzentrum
Cyber-SR	National Cyber Security Council	Nationaler Cybersicherheitsrat
CIT	Department Cyber/ IT	Abteilung Cyber/ IT
CNO	Computer network operation	Computer Netzwerk Operationen
CODE	Research Center Cyber Defence	Forschungszentrum Cyber Defence
CSD	Cyber Security Strategy for Germany	Cyber-Sicherheitsstrategie fuer Deutschland
GDP	Gross domestic product	Bruttoinlandsprodukt
EU	European Union	Europäische Union
Kdo	Command	Kommando
KdoCIR	Cyber and Information Domain Command	Kommando Cyber- und Informationsraum
KdoITBw	Army IT Command	Kommando Informationstechnik der Bundeswehr
KdoStratAufkl	Strategic Reconnaissance Command	Kommando Strategische Aufklärung
IT	Information technology	Informationstechnik

IT-ZentrumBw	Center for information technique of the Bundeswehr	Zentrum für Informationstechnik der Bundeswehr
NATO	North Atlantic Treaty Organization	Nordatlantikpakt
PPP	Public-private partnership	Öffentlich-private Partnerschaft
ZCSBw	Center for Cybersecurity of the Bundeswehr	Zentrum Cyber-Sicherheit der Bundeswehr
ZGeoBw	Geoinformation Center of the Bundeswehr	Zentrum für Geoinformationswesen der Bundeswehr
ZITis	Central office for IT in the Security Sector	Zentralen Stelle für Informationstechnik im Sicherheitsbereich

8. Bibliography

BMI, 2017. Startschuss für ZITiS [WWW Document]. Bundesminist. Inn. URL http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2017/01/zitis-vorstellung.html (accessed 8.10.17).

BMI, 2016. Cyber-Sicherheitsstrategie für Deutschland 2016. Bundesministerium des Innern, Berlin.

BMI, 2011. Cyber Security Strategy for Germany. Bundesministerium des Innern, Berlin.

BMJV, 2017. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) [WWW Document]. URL https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html (accessed 12.11.17).

BMVg, 2017. Konzept für die personelle Unterstützung der Cyber-Community der Bundeswehr („Cyber-Reserve“). BMVg, Berlin.

BMVg, 2016. Abschlussbericht Aufbaustab Cyber- und Informationsraum (Regierung). Bundesministerium der Verteididgung, Berlin.

BMVg, 2006. Weissbuch 2006 zur Sicherheitspolitik Deutschlands und zur Zukunft der Bundeswehr. Bundesministerium der Verteididgung, Berlin.

BSI, 2017. Das BSI-Gesetz [WWW Document]. URL https://www.bsi.bund.de/DE/DasBSI/Gesetz/gesetz_node.html (accessed 3.10.17).

Bundestag, 2017. Strukturen des Organisationsbereichs Cyber- und Informationsraum der Bundeswehr in Nordrhein-Westfalen: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Sevim Dağdelen, Christine Buchholz, Annette Groth, weiterer Abgeordneter und der Fraktion DIE LINKE. (No. 18/12277). Deutscher Bundestag, Berlin.

Auswärtiges Amt, 2017. Cyber-Außenpolitik. Auswärtiges Amt.

Die Bundesregierung, 2016a. White Paper 2016 on German Security Policy and the Future of the Bundeswehr. Bundesregierung, Berlin.

Die Bundesregierung, 2016b. Acht Prozent mehr für die Verteidigung [WWW Document]. URL https://www.bundesregierung.de/Content/DE/Artikel/2016/09/2016-09-07-etat-bmvg.html (accessed 5.11.17).

European Commission, 2017. Building an Effective European Cyber Shield - EPSC - European Commission.

European Commission, 2016. The Directive on security of network and information systems (NIS Directive). Digit. Single Mark.

NATO, 2014. Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. NATO.

Reinhold, T., 2017. Cyber-Fachkräfte-Initiativen bei der Bundeswehr. Cyber-Peaceorg.

Universität der Bundeswehr, 2013. Pressemitteilung: Neues Forschungszentrum CODE gegründet.

UP KRITIS, 2013. UP KRITIS: Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen: Grundlagen und Ziele.

Worldbank, 2017. GDP (current US$) [WWW Document]. URL http://data.worldbank.org/indicator/NY.GDP.MKTP.CD?year_high_desc=true (accessed 7.27.17).

The United Kingdom

Robert S. Dewar
Centre for Security Studies
ETH Zürich

Highlights/Summary

1. Key national trends

The UK is an important international actor in cybersecurity and cyberdefense. It works closely with US, NATO and European allies and is able to project both hard and soft power. The UK has placed cyberrisks as a high national security priority, including the protection of digital infrastructures. That being the case, the UK Cabinet Office – a civilian organ of the UK government – is the lead authority in UK cybersecurity policy. As such cybersecurity is approached from a civilian-led, resilience-focused standpoint, as ICT has historically been considered as a tool for economic growth and social improvement. From a leadership perspective, the UK's policy development framework occupies a position more towards centralization than decentralization.

2. Key Policy Principles

2.1. Cybersecurity

Cybersecurity for the UK means ensuring that the economic and social opportunities afforded by cyberspace are available to all with a minimum of risk to corporate, personal/citizen and national interests. Cybersecurity policy encompasses civilian, criminal justice and military/defense considerations. This solidifies the UK's civilian-led cyber policy while still addressing latent cyberrisks and ensuring the UK retains its position as a leading digital nation.

2.2. Cyberdefense

The UK does not have a dedicated or separate cyberdefense policy. Cyberdefense issues are addressed in the UK's cybersecurity strategy, with input from the National Security Strategy. As such the core cyberdefense principles are the protection of UK interests at home and abroad, but within a civilian cyber*security*-led policy framework. That being said, the UK has established a National Offensive Cyber Program to develop offensive capabilities. Because this Program establishes such capabilities within a deterrence framework, the UK's posture in cyberdefense can still be considered defensive rather than offensive.

3. Key national frameworks

3.1. Cybersecurity

Policy-making and overall leadership in cybersecurity comes from the Cabinet Office, specifically the Office of Cybersecurity (OCS). Operational actions – the actual securing of systems and infrastructure – come from Government Communications Headquarters (GCHQ – the UK's center for intelligence-gathering and security provision which operates under the Foreign and Commonwealth Office) and from the Ministry of Defense (MoD). The UK's cybersecurity structure is therefore a hierarchical structure with three main policy-making and operational centers.

3.2. Cyberdefense

The MoD focusses on the protection of its own networks and national defense, but no detail has published regarding the latter in terms of actions or capabilities in the cyber domain. The MoD also has no declared role in homeland security in the event of a major cyberattack affecting UK national systems and infrastructures.

4. Level of partnership and resources

The UK co-operates with core international allies such as NATO, the EU and the US and is a member of the Five Eyes intelligence-sharing partnership with the US, Canada, Australia and New Zealand.

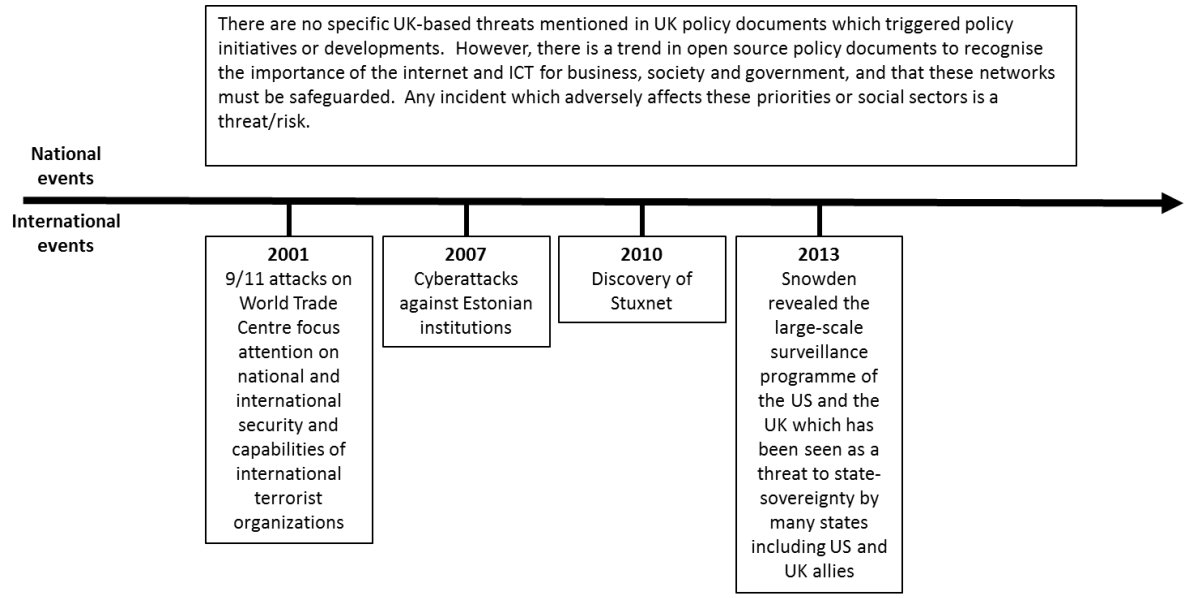
The UK actively promotes private sector partnership and involvement in cybersecurity (and by extension cyberdefense) provision, to the extent that it recognizes in policy that a significant portion of the UK's cybersecurity and defense tools and measures will be owned and operated by the private sector. There is, however, little specific detail provided regarding oversight or action.

1. Evolution of national cybersecurity policy (since mid-1990s)

1.1. Threat perceptions: trigger events

This section describes the main domestic and international events that had an impact on the shaping of cybersecurity and cyberdefense policies in the UK. NB: the international events listed are not specifically cited in UK policy documents but are referred to in interviews and media reports.

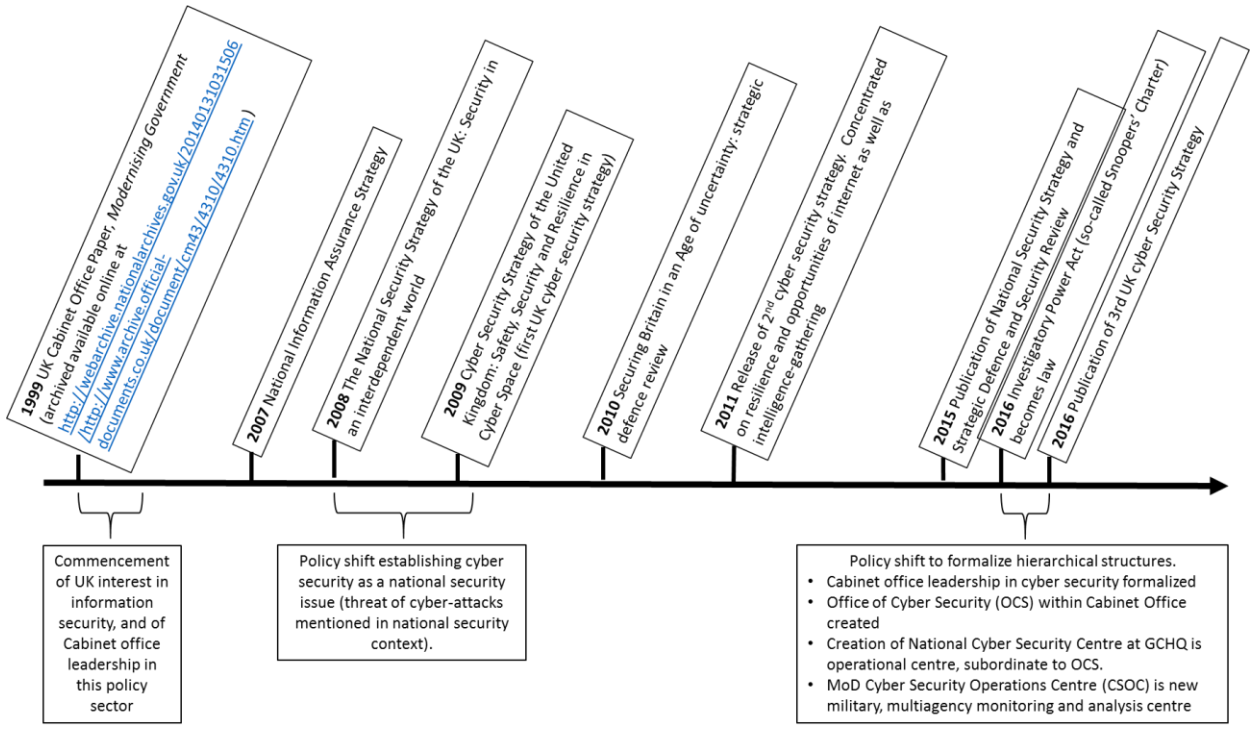
Diagram UK1: Timeline of Trigger Events



1.2. Main policy documents: Key shifts in strategy

This section describes the main policy shifts and trends identifiable in UK strategy, correlated with the publication of relevant policy documentation.

Diagram UK2: Timeline of Policy developments and Trends



1.3. Organizational structures: key parameters

The primary focus of UK cybersecurity and cyberdefense policy is one of a "grand strategy". The overall goal is to secure the UK's position in cyberspace – its ability to conduct and attract e-commerce as well as protect the national interest and UK citizens when online. Cyberdefense is a part of this overall cybersecurity strategy. The UK's Cabinet Office has overall strategic leadership of all aspects of cybersecurity: it has "has overall ownership of Cybersecurity Strategy" according to 2016 NCSS (p. 17)[41] through the Office of Cybersecurity (OCS) making cybersecurity policy civilian-led, centralized policy area. This position of overall leadership also places the Cabinet Office and the OCS above the UK Ministry of Defense (MoD) and results in a division of labor between policy-making and strategy development and operationalization.

Operational capabilities are further divided between the civilian and military, with a heavy weighting towards civilian leadership and oversight. The National Cybersecurity Centre provides UK-wide support and is hosted by GCHQ, an intelligence-analysis center under the oversight of the Foreign and Commonwealth Office (FCO). As such it has a civilian leadership, despite maintaining close co-operation with national security, military and intelligence bodies. In military operations, including offensive capabilities, the Cybersecurity Operations Centre based out of the MoD takes the lead. That being said, both of these bodies are subject to the Cabinet Office's overall oversight.

1.4. Context/Analysis: key national trends[42]

The UK has positioned itself as an important regional and international actor. It is an important player in European affairs and, until the Brexit vote in 2016, it was a leading voice in the European Union (EU). As a nuclear power is holds one of the five permanent seats on the UN Security Council, giving it the ability and authority to project itself in hard power terms. That projection includes defending its own territorial and international interests. The UK is also a member, along with the US, Canada, Australia and New Zealand – of the Five Eyes intelligence sharing program. In the field of cyberdefense, the UK is a member of and contributes to the work of the NATO CCDCOE in Tallinn. As such it is an active player in global security initiatives and operations. In soft power terms it is one of a number of centers of global finance, a member of the G7 group of industrialized nations and one of the largest providers of humanitarian aid.

It is in this field – soft power and promotion of economic interests – that the UK positions its cybersecurity strategy. Information and communications technologies (ICT) have historically been viewed as tools for economic growth and social improvement, rather than as corollaries of hard power. The protection of information and other digital assets is necessary to safeguard the UK's financial opportunities and protect digital assets. It is in this context that cybersecurity policy is developed.

Cyberdefense is developed as a component of cybersecurity, as a subsection of a grander strategy seeking to ensure the UK remains a safe, secure and resilient place to live and do business online. The UK's public rhetoric is not one of military cyberdefense posturing. UK cybersecurity and cyberdefense policy can be described as one which subordinates defense and military matters to social, governmental and business priorities. Civilian authorities therefore have the lead in both cybersecurity and cyberdefense areas given the oversight responsibilities of the OCS. On a spectrum of civilian versus defense-agency leadership, the UK clearly favors civilian overall oversight. This is further emphasized by military use of cyber capabilities being mentioned almost in passing or as footnotes. While there are oblique references to military use of cyberdefense tools (UK Government, 2015, p. 41), there is a clear desire to present the UK as a safe place live and work online and do e-business, with defense considerations coming second.

To achieve cybersecurity, and hence cyberdefense, the UK policy includes efforts at personal, regional, national and international level. Co-ordination efforts with regional partners in the UK (such as devolved assemblies) as well as international allies (such as NATO and the EU) are prioritized. As with other European states (e.g. Germany), the UK pursues a primarily civil-dominant approach with an acknowledged but bounded military dimension. Cybersecurity is therefore a component of UK national security but only in the sense that achieving cybersecurity will aid national security. Information infrastructures are "critical to national security" (UK Government, 2016, p. 37) and the UK government reaffirms the position that cyber threats should be considered as "Tier 1", the highest level of threat to the UK (UK Government, 2015, p. 13).

Of particular note is the fact that all responsible agencies, including the NCSC, the OCS, GCHQ and the intelligence services feed into cyber-intelligence activities – i.e. data gathering and analysis (UK Government, 2016, p. 28). The police and the military coordinate with each other to disrupt hostile foreign activity and cyber-criminality. While not made clear, it is implied that UK police handle criminal activity while the military focus on foreign activity. The NCSS provides a public face for all cyber activities, including those of a classified nature (UK Government, 2016, p. 29). The

[41] See glossary for a description of the Cabinet Office

[42] A 2011 report by the CCDCOE examines the background and current state-of-play (as at 2011) of UK cyber security policy, including defense matters. Although it does not cover the most recent developments, i.e. the 2016 UK NCSS, it provides detail on the background, development and structure of UK cyber security measures. Some info used here

relationship is, therefore, that systematic intelligence can facilitate cybersecurity, not that cybersecurity requires unlimited amounts of unfettered intelligence. This is perhaps a response to the Snowden allegations of 2011, where the UK intelligence services came under scrutiny for their practices of bulk data gathering.

UK cyberdefense policy is therefore a paradox. Cyberthreats are considered one of seven key national security priorities the UK must be prepared to defend itself (UK Government, 2015, p. 40). However, that defense is undertaken in the context of a non-military, prosperity-centric cybersecurity strategy, albeit with the development of offensive capabilities to act as a deterrent. This paradox reflects the UK's position both as a global financial leader, but also its commitment to military alliances and national security intelligence-sharing. Cybersecurity can therefore be seen as a microcosm of the UK's national security posture.

2. Current Cybersecurity Policy

2.1. Overview of key policy documents

2.1.1. The 2015 National Security Strategy and Strategic Defense and Security Review and 2016 Annual Report

Current UK national security policy can be found in two documents, the National Security Strategy and Strategic Defense and Security Review (NSS) published in 2015 and the Strategic Defense and Security Review (SDSR) published in 2016. These documents establish that cybersecurity policy and strategy is addressed in its own, separate policy document (UK Government, 2015, p. 40). Cyberdefense, however, is addressed without the requirement for a specific cyberdefense strategy. Instead, "cyber" issues are recognized in the 2015 NSS and 2016 SDSR as key aspects of the UK's wider national security policy.

In the 2015 NSS, the impact of technology, particularly cyberthreats, is one of four key security priorities for the coming decade (UK Government, 2015, p. 15). Cyber issues are prioritized alongside more traditional national security concerns such as terrorism, state-based threats, the "erosion of the rules-based international order" and serious and organized crime. This prioritization of cyber matters includes:

- The risks posed by both cybercrime and state-based cyber operations
- The development of cyber capabilities by states
- The development of cyber capabilities by non-state actors
- Cyber capability proliferation

Cybersecurity is therefore one of the highest security agendas for the UK. An important part of UK defense policy is to defend the UK and its territory. This includes airspace, territorial waters and cyber space (UK Government, 2015, p. 28). To achieve this, the NSS states that the Joint Cyber Group (JCG) will be one of the joint armed forces centers which will be developed in the future as part of maintaining the UK's military advantage.

From a practical perspective, the NSS stipulates that the UK Armed Forces will have strong cyber defenses including "offensive cyber capabilities" (UK Government, 2015, p. 41) developed as part of a National Offensive Cyber Program (NOCP), run in partnership with Government Communications Headquarters (GCHQ) and the Ministry of Defense (MoD). While not giving specific details on the nature of those capabilities or the range and scope of the NOCP, by explicitly stating its existence and the UK's preparedness to undertake offensive cyber operations, the NSS demonstrates the UK's commitment to a more active posture in cyberdefense.

Cybersecurity, and by extension cyberdefense issues, is a component of the threat posed by developments in new technologies. There are not a threat in and of themselves. Rather the threat is the capacity for state and non-state actors to deploy digital resources against UK critical national infrastructure and other national and international interests. To counter or mitigate this threat the UK will co-operate and share knowledge with allies, in particular NATO.

2.1.2. National Cybersecurity Strategy 2016

The current UK National Cybersecurity Strategy (NCSS) was published in 2016 and establishes UK policy until 2021. The document maintains the institutional subordination of defense considerations to civilian authority and control established in previous policy documents dating back to 1999 (see Diagram 2 above). Because the UK's NSS of 2015 makes clear that cyberdefense in the UK is a function or corollary of cybersecurity, the NCSS is the primary policy document for both cybersecurity *and* cyberdefense.

The NCSS establishes the policy-development and oversight hierarchy currently in place in the UK. The Office of Cybersecurity – based in the UK Government's Cabinet Office – is the policy and oversight hub for all cybersecurity and cyberdefense policy. In addition to establishing this oversight and policy development structure, the 2016 NCSS set out

the UK's core vision for cybersecurity up to 2021: that the UK be "secure and resilient to cyberthreats, prosperous and confident in the digital world". To achieve this vision, the Strategy has four core aims:

1. To defend UK against evolving cyberthreats;
2. To deter adversaries using the means to take offensive action in cyberspace should the need arise, in order to detect understand and disrupt hostile action;
3. To support industry and science to develop and maintain expertise to overcome current and future threats;
4. To achieve a free, open, peaceful and secure cyberspace through co-operation with other actors and entities and promoting multi-stakeholder internet governance.

According to the 2016 Strategy, cybersecurity (and hence cyberdefense) remains a function of the Cabinet Office with *support* from the UK's Ministry of Defense. The Cabinet Office therefore retains its position as the pre-eminent institution in UK cybersecurity policy and strategy development and leadership. This is emphasized by the fact that there is no specific or separate policy or strategy for cyberdefense in the UK. The vast majority of detail on cyberdefense measures is included in the NCSS document (see 2.2). It was in the NCSS that the National Cyber Security Centre at GCHQ and the Cyber Security Operations Centre at the MoD were initiated, but both remain under OCS oversight.

2.2. National cybersecurity strategy: fields, tasks, priorities

The NCSS states that the UK government's primary aim is to "make Britain confident, capable and resilient in a fast-moving digital world" (UK Government, 2016, p. 6). To that end the NCSS has four core objectives:

1. Defend the UK against evolving cyberthreats.

This involves ensuring UK networks, data and systems are protected as well as ensuring that citizens, businesses and the public sector can defend themselves. UK networks, data and systems in the private, commercial and public sectors are "resilient to and protected from cyberattack" (UK Government, 2016, p. 33).

There are a number of key components to this goal. Co-operation is vital to achieve this goal and the new NCSC at GCHQ will serve as an information and action hub. Active cyberdefense (ACD) is also a core component of UK policy in this regard. In UK policy, ACD is "the principle of implementing security measures to strengthen a network or system to make it more robust against attack" (UK Government, 2016, p. 33)[43]. The aim is to make the UK a harder target for criminal and state-sponsored activity as well as defeating malware intrusions. The NCSS states that the scope and scale of UK government capabilities to cause serious disruption to state-sponsored and criminal activities will be enhanced. As a corollary to the NCSS, the NSS Annual Report of 2016 reported that progress would continue to develop measures against high-level threats as well as high volume/low sophistication malware. This demonstrates the importance of cyberdefense in the national security context.

To achieve its defense goals in the context of cybersecurity the UK government will work with industry, especially Communications Service Providers, to thwart and disrupt attacks and their originators, and work to build a "secure by default" internet by ensuring greater supply-chain security (UK Government, 2016, p. 36) and building security measures into infrastructure.

2. Deterrence

This goal consists of using the means to take offensive action in cyberspace should the need arise, in order to detect, understand and disrupt hostile action. A lead is taken from the NSS, in that "defense and protection start with deterrence" (UK Government, 2016, p. 47). The aim is to dissuade and deter malicious actors from taking action against UK interests.

Although the NCSS states that deterrence is as applicable in cyber as in real world, reducing cybercrime is the first and most prominent goal, followed by "countering hostile foreign action" (UK Government, 2016, p. 49) and "preventing terrorism" (UK Government, 2016, p. 50) are the UK's key deterrence goals. It is significant that reducing cybercrime is positioned alongside hard security matters such as countering hostile foreign actors, and shows a recognition of the crucial difference between cybersecurity and other forms of security policy. The majority of malicious activity in cyberspace is criminal, and by tackling this aspect other potential malicious cyberactivity – even from a hard, national security perspective – can be reduced.

[43] ACD in the UK context therefore differs from other, more conventional definitions of the term. See Dewar, Trend Analysis 1: Active Cyber Defense (Dewar, 2017)

Despite this apparent law-enforcement focus, this section of the NCSS also contains explicit mention of offensive cyber capabilities. There is a National Offensive Cyber Program (NOCB) which seeks to develop offensive capability in cyberspace under the guise of the MoD and GCHQ. Developing capability and capacity in cryptography is also mentioned in this section. Separately, the 2016 NSS Review clarifies that ACD is a significant part of the NOCB work program.

3. Develop (UK Government, 2016, p. 54)

This third goal consists of supporting industry and science to develop and maintain expertise to overcome current and future threats. The primary focus is developing "home-grown talent" by advancing cybersecurity skills in schools and at all levels of the UK's education system. This will facilitate the stimulation of growth in the UK's own cybersecurity industry sector to create an "ecosystem" for industrial and academic development and a portion of the £165m Defense and Cyber Innovation Fund has been earmarked for this ecosystem.

4. The UK in the international sphere

The fourth section of the NCSS is not listed as a specific goal, but underpins the first three. It deals with the UK's action on the international platform and seeks to exploit the UK's perceived influence to "shape the global evolution of cyberspace" (UK Government, 2016, p. 9). The goal is to achieve a free, open, peaceful and secure cyberspace through co-operation with other actors and entities and promoting multi-stakeholder internet governance.

Although the application of current international law in cyberspace is advocated, the promotion of norms and patterns of good behavior, for example through the London Process of international conferences, are the primary goals of UK international cybersecurity policy. The principle of international co-operation also extends to cyberdefense, in which the UK aims to ensure that NATO is prepared for cyber conflicts.

2.3. National cyberdefense strategy: fields, tasks, priorities

As stated above, the UK does not have a dedicated cyberdefense strategy. Cyberdefense goals and aims are explored and tightly integrated into the NCSS and therefore are part of a grander cyber strategy. The 2015 NSS states that the Armed Forces will have strong cyberdefenses, and will be equipped to render assistance "in the event of a significant cyber incident in the UK" (UK Government, 2015, p. 41). This involves the use of offensive cyber capabilities – developed within the National Offensive Cyber Program (UK Government, 2016, p. 51) as part of "full spectrum of [UK] capabilities – to deter adversaries. A cyberattack will be treated as seriously as an equivalent conventional attack "and we will defend ourselves as necessary" (UK Government, 2015, p. 24).

However, at no *other* point in MoD policy is military assistance in cyberdefense mentioned. Even the areas listed on the MoD website where the MoD/Armed Forces will provide assistance to civilian or homeland agencies, cyber is not mentioned. There is therefore a disconnect between publicized cyberdefense policy in the context of it being a subsection of cybersecurity, and the operational reality pertaining to Armed Forces capability. It is unclear from open-source information which of the two situations is current operational UK policy[44] - whether the Armed Forces are committed to providing assistance in the event of a cyberincident or not. This makes it difficult to judge the level of involvement the UK military would take in the event of a major homeland cyberattack.

There is greater clarity in the UK's position on international cyberdefense. The UK aims to work with international partners, particularly in Armed Forces interoperability. NATO, Germany and the US are specifically mentioned as target partners in cyber activities. Given the UK's (current) position as a member of the EU and having a special relationship with the US, close co-operation with these major partners is not surprising. Nevertheless, the NSS reiterates the need to invest in home-grown talent and industrial bases for cyber development. This includes training and development.

2.4. Context/Analysis: key policy principles

The key principles in UK cybersecurity and cyberdefense policy and strategy are a civilian-led cybersecurity program incorporating the tools made available by various security agencies within a structured information-sharing and collaborating framework, in short, a grand strategy for cybersecurity. As discussed in Section 1.4, the UK's cybersecurity policy is a reflection of its wider approach to national security and its international position as both a hard-power and soft-power state. From the first National Information Assurance Strategy published in 2007, the UK government has maintained that the Internet and the digital domain are vital to the UK's economic, social and international interests

[44] This is perhaps not surprising given the covert or classified nature of certain potential capabilities.

(UK Cabinet Office, 2011, p. 7, 2009, p. 3, 2007, p. 1; UK Government, 2016, p. 6). The UK describes cyberspace as an interdependent network of information technology infrastructures including the Internet and the hardware that supports it. As such it is not a military domain *per se,* which means that the UK government's definition of the cyber realm conforms to its view of its importance as an economic and social entity. This view is further supported by the fact that, by 2016, the position and role of the UK, that of being one of the world's leading digital nations with a vibrant and safe online market place, had been acknowledged in policy and was one of the core roles to be secured.

This situation is reflected in the manner in which UK cybersecurity strategy is managed, with military and defense considerations – even from an operational perspective – being subordinated to the civilian authority based in the Office for Cyber Security at the UK Cabinet Office. This subordination is also reflected in the tone of descriptions of cybersecurity threats. Such threats are perceived first and foremost as civilian or commercial risks given the interconnected nature of UK businesses and society, rather than existential threats to the nation. There is a recognition that the majority of cyberincidents are carried out for criminal gain rather than for military or strategic advantage. Such possibilities are not discounted, and the military/MoD are given resources to combat those. While hostile action was present in earlier iterations of the NCSS, the 2016 version explicitly states that the UK has the tools, capabilities and willingness to take offensive action should there be a need to do so. Nevertheless, the priority for UK policy and strategy remains one of maintaining functioning services and infrastructure for national social and economic benefit. This policy choice enjoys a strong institutional continuity or path dependency. Important international events such as Estonia 2007, Georgia 2008 or the discovery of Stuxnet in 2010 have not shifted UK cybersecurity/cyberdefense structures to a more defense-oriented position.

This is not to say that cyberdefense is not considered important or is somehow relegated to a sideshow. The establishment of a National Offensive Cyber Program is testament to the UK's willingness to engage in military operations in cyberspace. However, the limitations and restrictions of that Program can be inferred from the fact that the UK does not have a dedicated, separate cyberdefense strategy. It simply means that the notion of civilian oversight of any military capability or program of capability development remains strictly under civilian oversight.

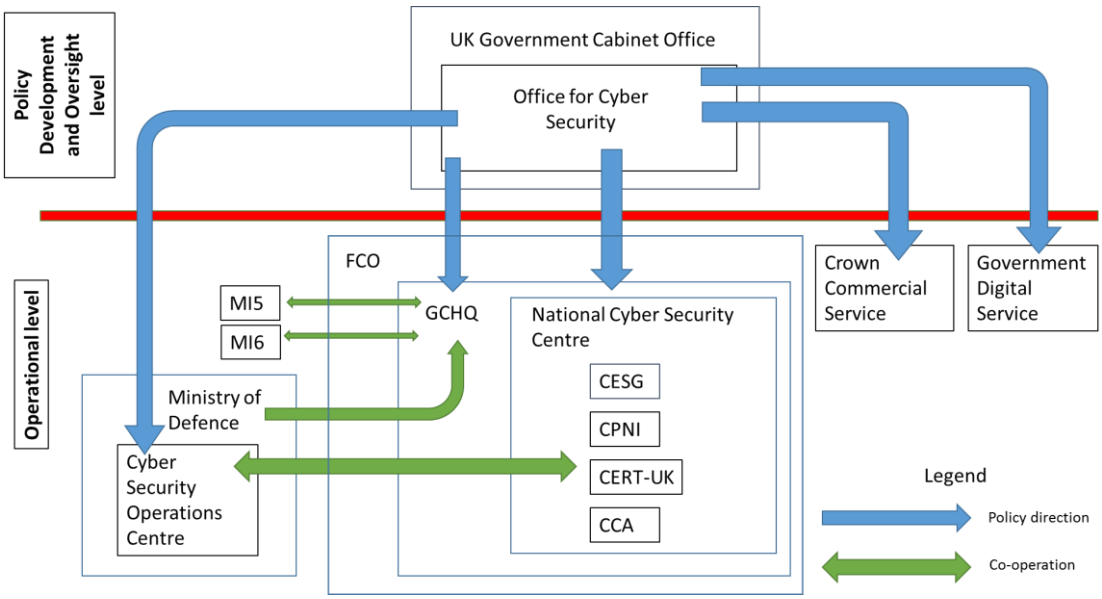
Of note is the fact that operational and co-operative partners listed include BRICS states. These are not traditional security partners for the UK, nor do they share the same long-standing, developed relationships such as those with NATO or the US. In recent years, however, BRICS countries, particularly China, South Korea and India, have demonstrated an increased capacity and capability in cyber matters, both in offensive and commercial capability. It is therefore logical that the UK court these states for co-operation.

3. Current Public cybersecurity structures and initiatives

3.1. Overview of national organization framework

Diagram 3 below provides a graphical representation of the organization of the UK's cybersecurity apparatus.

Diagram UK3: Oversight Organigram



3.2. National cybersecurity structures and initiatives: organization, mandate, legal aspects, operational capabilities

The 2016 NCSS establishes a list of roles and responsibilities for various agencies and ancillary bodies involved in ensuring, if not providing cybersecurity. This includes bodies in the intelligence community as well as three sectors of society:

- **Individuals** – private citizens need to take practical steps to ensure cybersecurity, including good cyber hygiene
- **Businesses and organizations** – These entities should ensure that their services and assets, particularly those that utilize private data, are appropriately secured. *There is also confirmation that if a business or organization is the victim of a cyberattack, then they are liable for the consequences.*
- **Government** – ultimately responsible for assuring national resilience and maintaining essential services

Operating alongside the UK's civilian security and law enforcement agencies are the **Security Service** (MI5) and the **Secret Intelligence Service** (MI6). These agencies share information and resources with GCHQ and the NCSC but, because they have very specific and exclusive intelligence-gathering remits, are operationally separate from the other bureaux and agencies handling UK cybersecurity. Due to their expansive remits they do not have a specific cybersecurity/cyberdefense function unless any of their specific tasks include such a function. Precise details of their actions, operational capabilities and interaction with other agencies is not available in the public domain due to the classified and sensitive nature of these agencies' work.

What follows is an examination of the various agencies and government entities involved in cybersecurity and cyberdefense. The framework developed by the UK divides responsibility in this field between, on the one hand, policy-development and overall leadership, and operationalizing that policy on the other. This division of remits is shown in Diagram 2 above.

3.2.1. The Cabinet Office and the Office of Cybersecurity (OCS)

Throughout the 1999-2016 timescape and beyond the **UK Cabinet Office** has overall strategic leadership of cybersecurity policy and implementation of that policy. As a result it does not operationalize policy but provides leadership. UK cybersecurity/information assurance policy originated in Cabinet Office paper of 1999 and continued to

be formalized in successive NCSS documents. Policy in all other cybersecurity issues (civilian, military, SIGINT, national security, terrorism, cybercrime) stems from Cabinet Office. Although this may be the result of institutional path dependency, the ongoing placement of leadership in cybersecurity at the Cabinet Office infers that cybersecurity is a civilian, non-military concern for UK government. There is a definite subordination of defense to civilian control, something present in earlier NCSS versions (see CCDCOE report) and confirmed in the 2016 NCSS. From 2016 the **Office of Cybersecurity** (OCS) *within* the Cabinet Office has led on cybersecurity issues.

3.2.3. Government Communications Headquarters (GCHQ)

Government Communications Headquarters (GCHQ) is the UK government's intelligence analysis center. It provides signals intelligence and information assurance analysis to the UK government, UK law enforcement agencies and national security and defense bodies. Although it works closely with military intelligence, GCHQ is a civilian agency under the oversight of the UK's Foreign and Commonwealth Office (FCO). Under the terms of the 2016 National Cybersecurity Strategy, GCHQ also hosts new National Cybersecurity Centre.

3.2.4 The National Cybersecurity Center (NCSC)

The **National Cybersecurity Centre (NCSC)** is the operational lead for UK cybersecurity and cyberdefense and is hosted by GCHQ. It is the National Technical Authority for responding to cyberthreats to the UK at macro level. Due to the range of offices and departments under its aegis, the NCSC is able to provide research and intelligence-based analyses on information assurance and threat assessments for policy development as well as provide direct advice on cyberterrorism and cyberespionage to public and private entities and national infrastructure providers.

The NCSC is designed to be a one-stop-shop for all the UK's cybersecurity and cyberdefense policy, analysis, intelligence-gathering and operations. As such it includes within its structure four specialist sections and agencies:

- The **Communications-Electronics Security Department** (CESG) is "the National Technical Authority for Information Assurance within the UK. It provides a trusted, expert, independent, research and intelligence-based service on information security on behalf of UK the government" (NCSS 2016 p. 73).
- **Centre for the Protection of National Infrastructure** (CPNI) focuses on the provision of vital services and provides advice aiming to reduce and minimize the vulnerability of national infrastructure organizations to terrorism and espionage. To achieve these aims in a cybersecurity context, the CPNI also work in partnership with the NCSC to provide "holistic protective security advice on threats from cyberspace" (NCSS 2016 p. 73).
- The **Centre for Cyber Assessment** (CCA) is also based within the NCSC and provides cyberthreat assessments for UK government departments to inform policy development (NCSS 2016 p. 73).
- The **UK Computer Emergency Response Team** (CERT-UK) provides direct, real-time support to UK government and infrastructure entities when major cyberincidents occur.

3.2.5. Ancillary agencies

Also separate to both the GCHQ-led NCSC and the MoD's agencies are the **Government Digital Service** and the **Crown Commercial Service** (p. 37 2016 NCSS). Although they are part of the UK's wider grand strategy for cybersecurity these organizations are not part of national cybersecurity analysis and response system. Instead they are intended to ensure government services are secure by default when digitalization occurs.

3.3. National cyberdefense structures and initiatives: organization, mandate, legal aspects, operational capabilities

Because cyberdefense is a subordinate section of the UK's cybersecurity strategy, much of cyberdefense policy is addressed in the UK's Cybersecurity Strategy (see Sections 2.2 and 3.2 above). This is also reflected in the references in this document to the National Offensive Cyber Program. Although this program is designed to develop offensive cyber capabilities, it does so under the policy aegis of the Cybersecurity Strategy and the National Security Strategy, rather than as an independent cyberdefense policy area.

Cybersecurity is a vital component of UK defense policy and capability according to the NCSS of 2016, therefore ensuring cybersecurity is primary aim of cyberdefense. This position is a reiteration of the position set out in the NSS of 2015. It is, however, beneficial to clarify that the UK's MoD leads on armed forces cyber capabilities (CNO and other activities relating to state-on-state cyber warfare). As with detail on the operation and capability of the UK's intelligence services, precise details relating to the UK's military capabilities is not available from public, open-source data, beyond

the statement that such capabilities exist, are necessary and are an important part of the UK's defenses. That being the case, the UK's MoD has established a military agency separate to the NCSC, the Cybersecurity Operations Centre.

3.3.1. Cybersecurity Operations Centre

Separate to NCSC and under direct remit of the UK's MoD is the **Cybersecurity Operations Centre (CSOC)**. The CSOC is a military, multiagency monitoring and analysis Centre (NCSS 2016 p. 10, 38) based at Corsham[45]. This agency has developed from 2009 into a MoD-supported unit.

3.4. Context: Key public organizational framework

As with all UK cybersecurity policy and strategy, from an operational perspective cyberdefense falls under the wider remit of cybersecurity. This entails a civilian oversight of armed forces capability and capacity, including the development and deployment of offensive cyber capability under the NOCP. Although such tools are available and others are being developed, because of this subordination to the priorities of the NCSC, the strategic context of action against hostile actors in cyberspace is also subordinated to wider cybersecurity priorities of maximizing the social and economic potential of cyberspace and protecting national assets. From a policy perspective and, to a certain extent, an operational perspective, this defensive, resilience-focused posture makes good sense: cybersecurity affects all areas of government, social and commercial life and a central oversight authority can provide leadership, policy and strategy direction in a whole-of-society, approach with centralized oversight and operationalization.

There are, however, some potential problems for this approach. An example of the pitfalls of centralization can be seen in GCHQ, especially given that body's numerous masters and stakeholders. The NCSC and GCHQ are answerable both to the new OCS in the Cabinet Office *and* the Foreign and Commonwealth Office. In the case of a major cyber incident on mainland UK, GCHQ and its NCSC run CERT-UK, the UK's internal, national cybersecurity response unit. These are civilian organs of government and the OCS is center of UK cybersecurity policy and strategy. For intelligence gathering and analysis GCHQ and the NCSC liaise with MI5 for homeland security and MI6 for foreign intelligence. Separately, for military intelligence and offensive capabilities GCHQ and CSOC liaise with the MoD, the CSOC and military intelligence agencies. The result is a tangled web of responsibilities and overlapping remits, including a blurring of the lines between civilian and military operational capability and action given that GCHQ and the NCSC work on *both* military *and* civilian cybersecurity issues.

The centralizing zeal of the OCS at the Cabinet Office is logical: it makes sense to have one national center focusing on cybersecurity issues, responses and capabilities. But the vast range of cybersecurity/cyberdefense issues and the differing levels and classification of intelligence could make such centralization problematic. The OCS is required to wear numerous "hats" depending on the issue at hand. If a cyberattack occurs a policy decision must be made as to whether the civilian disaster response hat is worn or the military-defense hostile foreign action hat is worn. That decision is a political one but how this decision is made, or who makes it, is not clear from the NCSS.

There are two results from the involvement of these numerous parties and their different goals. First, it makes placing the cyberdefense capabilities of UK on a spectrum of offense vs defense challenging. Explicitly mentioning offensive cyber capabilities as part of a national security framework ostensibly places the UK in the "offense" camp. However, information on those capabilities is sparse and, in any case, the development and deployment of those capabilities is strictly controlled by civilian entities. The UK therefore occupies something of a middle ground in the offense-defense spectrum. The second result of the involvement of numerous agencies in cybersecurity and cyberdefense is that the effectiveness of the UK's plans for centralization remains to be seen. The 2016 NCSS and the structures it instituted are indeed more streamlined and coherent than previous strategy documents, as was intended, but the different aims, goals and effective levels of information-sharing, including classified data, means that streamlining and centralization may not be as effective or successful as envisaged.

[45] See https://www.gov.uk/government/news/defense-secretary-announces-40m-cyber-security-operations-centre

4. Current cyberdefense partnership structures and initiatives

It is widely recognized that cybersecurity is a global issue. The nature of the Internet and the World Wide Web mean that information and data, malicious or otherwise, can be accessed from anywhere in the world and sent to anywhere else in the world. Just as cybersecurity and cyberdefense have global remits, every actor – state, corporate or individual – who has an online presence should take account of cybersecurity issues.

The analysis in this section of the Snapshots looks at those initiative aimed at developing partnerships and raising awareness. In the main, it examines the initiatives and structures relating to cybersecurity. In the case of the UK this is due to the fact that there is very little publically available information on measures specifically aimed at cyberdefense. That being said, given the intricate and subordinated relationship between UK cybersecurity and cyberdefense from a policy perspective, any initiatives aimed at improving cybersecurity at the individual, local, regional, national and international levels are intended to feed into national cyberdefense.

4.1. Public-private cybersecurity

According to the NCSS and previous strategies, co-operation between the public and private sectors is crucial to achieving cybersecurity goals, and only the UK government can take the initiative and drive that co-operation. It does this by encouraging investment in an "innovative UK cyber sector, if necessary through regulation and, where government systems and agencies develop new tools, these will be offered, where possible, to the private sector and the citizen". The UK is therefore very open about the need for the private sector to be involved in UK cybersecurity, particularly in the field of protecting critical national infrastructure (CNI). The UK's policy states that CNI must be resilient to cyberattack.

However, while the hardware and software which makes up the physical components used to host the Internet and the World Wide Web are to be secured, *providers* of information services are not yet considered part of the group of companies and organizations within the public and private sector which constitute critical infrastructure. Part of the reason for this omission is that the UK government will not take on responsibility to manage the risks to the private sector which emanate from cyber space. UK policy is explicit that this responsibility lies with the boards, owners and operators of the private entities themselves.

While this position is intended to mean that government is not responsible for the cybersecurity of private corporations and their infrastructure, UK policy is slightly ambiguous on this point. An initial reading of this statement seems to infer a contradiction with another policy statement: that ultimate national cybersecurity responsibility lies with the government. The UK government recognizes that, although key sectors of economy and cyber infrastructure are in private hands, the government is ultimately responsible for "assuring their national resilience and…maintenance of essential services." (UK Government, 2016, p. 27). There is a disconnect between, on the one hand, acknowledging the government's responsibility to ensure the safety of its citizens and national infrastructures (digital or otherwise) and on the other hand not becoming involved in the decisions of private companies.

One crucially important point to note is with regard to cyberdefense. Although the UK government acknowledges its responsibility for keeping the nation and its citizens safe, it states in policy that national cyberdefense capabilities – measures to "actively defend ourselves against cyberattacks" – will be developed and operated by the private sector (NSS p. 40). How the UK government reconciles managing the cyberrisks to the nation and society with the capabilities to do so being in private sector control is not made clear in public policy. It appears to establish a precedent for the privatization of cyberdefense. At the very least this statement is an acknowledgement of an important role to be played by private sector resources in cyberdefense provision, but one which does not establish the parameters of that role.

4.2. International cybersecurity partnerships

Section 2.3 above examined the international partnerships of greatest importance to the UK according to public policy statements. This includes working with traditional and long-standing allies and partners such as the US, NATO and the EU. What is surprising, however, is the list of countries specifically mentioned as current or potential in wider international co-operation. In addition to the EU in general, these partners are:

- South Korea,
- China,
- India,
- Brazil

This particular list of countries indicates that current UK policy is looking east as well as seeking to maintain links with traditional Western partners. The targeting of co-operation with BRICS countries indicates a willingness on the

part of the UK to expand its area of involvement outside of its traditional sphere of influence and operation and indicates where the UK government believes future investment and involvement would be most fruitful. There is no indication of a preference for military over economic alliances. Instead a preference can be inferred for building alliances and co-operation with actors of strategic *influence* in certain regions.

4.3. Cybersecurity awareness programs

Throughout the UK's current cybersecurity policy there are a number of awareness programs targeted at various sectors of society. These include:

- Cyber Aware (formerly Cyber Streetwise) – gives public advice on protecting themselves including strong passwords and regular security updates of software
- Cybersecurity Challenge – competitions for young people to test skills and consider "a career in cyber"
- Cyber Essentials – aimed at organizations protecting themselves against low-level "commodity threat"
- Get Safe online https://www.getsafeonline.org/ - free advice from UK government on how to use the internet safely on a range of topics and devices, including smartphones and tablets
- "10 Steps to Cybersecurity" – program instituted and sponsored by the NCSC. While Get Safe Online caters to private citizens, 10 Steps is aimed at organizations and raising awareness at corporate board level.

4.4. Cyberdefense education and training programs

There are no specific education and training programs in the field of cyberdefense which have been made public. That being the case, some of the programs listed in Section 4.3 above, such as the Cybersecurity Challenge, can facilitate the identification of individuals with particular talents or skills sets which may be of benefit. An additional scheme for such a purpose is the Cyber First undergraduate sponsorship scheme. This is a government-backed scheme run by GCHQ aimed at identifying talented young people with a view to training them as cybersecurity specialists. Undergraduate tuition at university is paid for and a three-year national security job is available on completion of the university degree.

5. Annex 1: Policy Spectra

These sliding scales represent three policy spectra:

1. The extent to which policy development and management in cyberdefense and cybersecurity is centralized;
2. The extent to which these areas fall under civilian or military oversight and
3. Whether or not the state under examination has a defensive or offensive cyberdefense posture.

As set out in the introduction to this collection, a state's position on these sliding scales is derived from the analysis in the snapshots. For example, if a state concentrates a significant amount of policy development and implementation responsibility in only a few or a single entity, it is reasonable to conclude that that state operates a more centralized approach to cybersecurity and defense leadership. Similarly, if responsibility in these sectors is placed in the defense ministry then there will be a greater degree of military rather than civilian oversight, and if the possession of offensive cyberdefense capabilities is explicitly stated in the policy literature, a state can reasonably be said to maintain an offensive cyberdefense posture, even if specific capabilities and tools are not mentioned.

5.1. Centralization vs Decentralization of Leadership

Diagram UK4: Spectrum of Centralization vs Decentralization of policy development and management

Centralized control -----X---------- Decentralized control

5.2. Civilian vs defense posture and oversight

Diagram UK5: Spectrum of Civilian-Defense cybersecurity posture and oversight

Civilian oversight -----X---------- Defense

5.3. Offensive vs defensive capabilities

Diagram 6: Spectrum of Offensive vs Defensive cyberdefense capabilities

Offensive----------X---------- Defensive

6. Annex 2: Glossary of Terms and Key Definitions

Term	Definition
Active cyberdefense	In the UK policy context, ACD "is the principle of implementing security measures to strengthen a network or system to make it more robust against attack".
Cyberattack	The deliberate exploitation of computer systems, digitally-dependent enterprises and networks to cause harm
Cyberincident	An occurrence that actually or potentially poses a threat to a computer, internet-connected device, or network – or data processed, stored, or transmitted on those systems – which may require a response action to mitigate the consequences
Cyberresilience	The overall ability of systems and organizations to withstand cyber events and, where harm is caused, recover from them
Cybersecurity	The protection of internet- connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorized access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so.
Cabinet Office	A Department of UK Government which supports the UK Prime Minister and ensure the effective running of government. The Cabinet Office is also the corporate Headquarters for government, in partnership with HM Treasury, and we take the lead in certain critical policy areas. The Cabinet Office is a ministerial department, supported by 18 agencies and public bodies. (Source: https://www.gov.uk/government/organisations/cabinet-office)

7. Annex 3: Abbreviations and acronyms

Abbreviation/Acronym	Name
BRICS	Emerging economies of Brazil, Russia, India, China and South Africa
CCA	Centre for Cyber Assessment
CCDCOE	Co-operative Cyber Defense Centre of Excellence
CCS	Crown Commercial Service
CERT-UK	UK Computer Emergency Response Team
CESG	Communications-Electronics Security Department
CNI	Critical national infrastructure
CPNI	Centre for the Protection of National Infrastructure
CSOC	Cyber Security Operations Centre
EU	European Union
GCHQ	Government Communications Headquarters
GDS	Government Digital Service
JCG	Joint Cyber Group
MI5	UK Security Service
MI6	UK Secret Intelligence Service
MoD	Ministry of Defense
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Centre
NCSS	National Cyber Security Strategy
NOCP	National Offensive Cyber Program
NSS	National Security Strategy and Strategic Defense & Security Review
OCS	Office of Cybersecurity

8. Bibliography

Dewar, R.S., 2017. Trend Analysis 1: Active Cyber Defense.
UK Cabinet Office, 2011. The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.
UK Cabinet Office, 2009. Cyber Security Strategy of the United Kingdom: Safety, Security and resilience in cyber space.
UK Cabinet Office, 2007. A National Information Assurance Strategy.
UK Government, 2016. National Cyber Security Strategy 2016-2021.
UK Government, 2015. National Security Strategy and Strategic and Defense Review.

Summary of Findings and Conclusion

Robert S. Dewar
Centre for Security Studies, ETH Zürich

Cybersecurity and cyberdefense policy is approached differently by different nation states. This is due to different institutional structures and idiosyncrasies in states' historic approaches to these policy areas. Nevertheless, there exist certain similarities in policy development frameworks and operational architectures: there are trends towards civilian leadership and oversight, and building institutional structures prior to policy development. A particular interest for this first collection of national snapshots has been how cyberdefense and cybersecurity are treated as policy areas by the different nations researched. This includes examining such areas as where cyberdefense sits between civilian and military government offices, how cybersecurity and defense policy is operationalized and the impact of separating cyberdefense from wider national security policy. The ongoing exercise of developing "live" national policy snapshots, and updating each examination in successive editions of the collection, will facilitate the long term goal of the CSS of developing a typology of best practice in a dynamic policy area.

Creating the snapshots works towards not only examining the trends, differences and commonalities in cybersecurity and cyberdefense policy, but in future will also enable us to develop typologies in policy development, for example the types of organizational structure most frequently employed in these fields, which type of agency (civilian or military) takes the lead role in the field or the preferred position of operational agencies within a policy architecture.

The comparison of national policy snapshots in this first edition yields a number of findings ranging from general trends in policy development across the case studies, to national idiosyncrasies relating to the level and nature of policy centralization. The most significant of these findings are summarized here.

1. Evidence of a process of transformation

At the general level, the snapshots confirm a process of transformation in policy priorities. Nation states are systematically formulating cybersecurity and cyberdefense strategies to counter perceived global cyberthreats and digital risks. As a result of the importance of digital networks and the infrastructures which use them to the continued functioning of a state, the policies and strategies being developed are interconnected – either implicitly or explicitly – with national security strategies. Where there are differences between the solution-building approaches and prioritization of risk between the national frameworks, these differences are due not to a lack of awareness of those risks but, in large part, to differences in the internal structural and decision-making systems of the states examined. Path dependencies established in earlier policy choices – terminology and conceptualizations, positioning of cybersecurity within a civilian or military context – remain in place and continue to exert a strong influence. This policy inertia further entrenches national idiosyncrasies.

Another characteristic of this process of transformation is that states have been observed establishing policy-development and operational frameworks and structures which incorporate several different organs of government. This has led to an observable increase in clarity in national policy-development structures, despite variance in those structures across the states examined. Interior ministries and prime ministerial offices are working alongside military apparatus (such as defense ministries and army commands) to develop strategic responses to cybersecurity threats. Cybersecurity is often approached in a holistic manner, an overarching framework which includes low-level cyber-crime[46] as well as national security implications. Cyberdefense is more commonly applied as a facet of national security. It concentrates on ensuring national digital infrastructures and the physical systems that rely on them are free from internal and external malicious disruption. Cyberdefense also includes ensuring that military and national security agencies have the digital resources needed to carry out their responsibilities, including offensive capabilities.

2. Precise policy remains vague

The clarity present in policy-development or operational government structures is not, however, being extended into policy itself. Cybersecurity and cyberdefense remain ill-defined and inconsistently applied concepts and the policy documents produced remain vague on specific policy details and solutions. An important reason for this vagueness is a lack of consistent or defined nomenclature. There are a number of national conceptualizations and definitions published by state policies and strategies, conceptualizations as diverse as the national perspectives and priorities they reflect. While "cybersecurity" is a popular term in the media, policy jargon and civilian discourse, a number of states

[46] Online criminal activity which does not threaten national security

substitute "digital" for "cyber" while still referring to the same issues as their international partners. At one level this is to be expected. With the establishment of a policy-development framework which incorporates all interested government parties – military and non-military alike – a government will subsequently have the expertise in place to ask: what are the main cybersecurity risks and how does we mitigate them? A systemic consequence of this process, however, is that national priorities, path dependencies and vagaries in national political and strategic culture inevitably play a role in defining cybersecurity and cyberdefense.

This lack of standardized nomenclature creates difficulties for analysis as well as contributing to the overall conceptual and definitional fog which continues to surround cybersecurity and cyberdefense. This demonstrates a lack of maturity of definitions. Future editions of this collection will, it is anticipated, serve to alleviate this lack of clarity by identifying core ideational traits common to most if not all national conceptualizations of these terms.

It is worth noting, however, that the vagueness and perceived weakness of policy also stems from the fact that only open-source policy documents were analyzed for this collection. States are understandably reticent to publicize details on capabilities and specific technical solutions. This is particularly problematic with those states where cyber defense is positioned within national security or defense policy frameworks. Details on capabilities, and the capabilities themselves, tend to remain classified and not published in open-source policy documents or analyses.

3. Centralized policy implementation frameworks are built *before* policy is developed

A consequence of the vagueness of national policy is that there is a tendency for states to build their policy-making and implementation organizational frameworks first, *and then* to develop policy. States establish units or agencies with responsibility for cyber security and defense within government ministries and then task them with developing policy in those areas. At first glance, it would appear that this tendency is occurring *despite* vague and weak conceptualizations of the policy problems. The reality, however, is that these structures are being developed *because of* this vagueness. Nation states are gathering together expertise and experience in these fields with the object of identifying, developing and implementing policy solutions. In the case of implementation of policy, there is a clear tendency towards developing specific organs of government and new public bodies to provide information and/or practical assistance in preventing cyberincidents taking place, or providing rapid-response resources in the event of an incident.

There are two further consequences of this tendency to build organizational structures before developing policy. The first is an observable trend towards centralizing leadership and oversight in cybersecurity and cyberdefense. This is being carried out to reduce the fragmentation of responsibilities and remits and streamline both policy development and operational processes. The second is that, when centralized structures and frameworks of co-operation are established, oversight and leadership responsibilities for both cybersecurity *and* cyberdefense tend to gravitate towards non-military – i.e. civilian – ministries, offices, agencies and bureaux. For cybersecurity this makes logical sense given that the vast majority of malicious cyber activity is criminal in nature. However, for cyberdefense this gravitation *away* from military leadership and oversight is somewhat unexpected given the national security rhetoric surrounding it. Even in those few examples where intelligence and military agencies have operational oversight of cyberdefense – such as the UK – the agencies themselves fall under the aegis of foreign or interior ministries and *not* defense ministries. Furthermore, overall leadership in this sector stems from civilian entities. For *both* cybersecurity and cyberdefense this demonstrates a trend towards holistic, *civilian* oversight of these policy areas, despite the strong interconnection of cyberdefense with national security and defense strategy.

While the pooling of expertise to create efficient policy development structures is neither surprising nor novel, it is noteworthy that this centralization occurs at a high level of government. It occurs at or just below prime ministerial level. The positioning of cybersecurity and cyberdefense considerations at such consistently high levels of government demonstrates the importance placed upon these policy sectors by the states examined.

There are, however, certain important differences in the nature of centralization, particularly as regards the operationalization of cybersecurity and cyberdefense policy and the support provided to the state by key responsible agencies. The nature of that support differs depending on which type of agency is given the larger role or wider remit. For example, in the UK, direct assistance when a cyber incident occurs is provided by CERT-UK, a unit of GCHQ. This is a national security agency with strong ties to the military, but one which has civilian oversight from the UK's Foreign Office. This can be contrasted with, for example, the French system, where operational support and incident-response assistance for critical infrastructures comes from the ANSSI – a civilian body – under the supervision of the Prime Minister's office. The function of both these bodies – GCHQ and ANSSI – is similar given the need for assistance, both in terms of incident prevention and incident response. However, the nature and tenor of that support will differ given the different institutional natures and architectures of the two agencies.

4. Recognition that "cyber" as a concept is important for national socio-economic as well as defense purposes

The trend towards positioning cybersecurity and cyberdefense policy oversight and leadership in civilian organs of government reflects a trend in recognizing the importance of both of these areas not just to a state's national security, but to its socio-economic wellbeing. Due to the high level of connectivity at all levels of a state's government, economy, society and industry, cybersecurity threats and risks can and do affect all areas of a nation state. Furthermore, statistically speaking, the vast majority of cyberincidents are criminal in nature and therefore have widespread socio-economic effects, such as reducing citizen trust in digital systems. Securing the nation means not just protecting critical infrastructure and defending national interests, but also preventing, mitigating or reducing the social fallout from major cyberincidents, a fallout which may be of more direct consequence to individual citizens than to critical national infrastructure.

This recognition of the potential for a whole-of-society impact of a cyberincident demonstrates an application of the principles of grand strategy to cybersecurity and cyberdefense. As discussed in the Introduction to this collection, "grand strategy" is the co-ordination and direction all of the resources of a state, or group of states, towards achieving security (Liddell Hart, 1967). This principle – the commitment of all of a state's resources – is being increasingly applied in state cybersecurity policy. Due to the ever-increasing penetration of digital and Internet-enabled technologies in all walks of social, political and economic life, cybersecurity is of importance to all aspects and sections of a state. Solutions, however, need to be just as holistic and so all resources and capabilities available to a state are being committed to achieve cybersecurity. In addition, not only are all the resources and component parts of a state geared towards ensuring national cybersecurity (a grand strategy concept) but cybersecurity and cyberdefense policy must also ensure that all those component parts are protected. To coin a phrase, cybersecurity – including cyberdefense considerations – is becoming an issue where "grand security" is being applied: all the resources of a state, or group of states, are being committed to the attainment of security.

5. Centralization is a work-in-progress

Despite steps being taken to tackle fragmentation in cybersecurity and cyberdefense by establishing clear policy development structures and centralizing those structures around high-level organs of government, there still remains an ongoing and fluid definition of those responsibilities. In some cases, notably France and the UK, a number of institutional changes have occurred between current and previous internal structures. While some of these changes represent changes in prioritization due to incoming administrations bringing with them different political goals, others have been more fundamental, leading to the establishment of new offices with expanded remits. This further highlights core differences in the nature of centralization: it can be either *expertise-driven* or *remit-driven*. Where centralization is *expertise-driven* the nature of that centralization favors gravitating towards already-existent centers of expertise. An example is the centralization undertaken by Germany and the UK. In both cases, rather than reinvent the wheel, a center of excellence already operating in a particular policy sector – the BSI in Germany and the UK's GCHQ – is given an expanded remit and tasked with operationalizing that policy. Conversely, centralization may be *remit-driven*. An example can be found in France's approach. Here cybersecurity and cyberdefense were to have clear civilian oversight and leadership. As a result a new civilian entity, separate to the intelligence services and military, was established to operationalize French policy within a civilian-led remit.

There are advantages and disadvantages to both approaches. On the one hand, by taking an expertise-based focus, a government is utilizing resources already in place to even greater advantage. Those resources, however, may bring certain conceptual baggage to the operationalization of policy, particularly if, historically, the office in question has been a tool of the military. Establishing a completely new entity may therefore be more pragmatic if "grand security" is to be achieved (see Point 5 above). That being said, the expertise must come from somewhere. It must either be drawn from other government agencies, thereby disadvantaging those agencies, or drawn from outside government circles, such as the private sector. However, attracting and retaining private sector expertise is both challenging and costly.

This fluidity mirrors the challenges faced in cybersecurity in general. The technology underpinning cyberspace, and the security threats that that technology can bring, are in a constant state of flux and innovation. Policy responses must respond to new threats leading to a necessary level of policy and operational flexibility. Nevertheless, the number of changes and shifts in designation of national responsibilities indicates that in most cases this is still not settled.

6. Developing cooperative networks with traditional and non-traditional security actors

In the main, the countries examined in the collected snapshots pursued economic and military partnerships with traditional organizations. Multilateral bodies such as the EU, NATO, the OSCE and OECD were frequently represented.

Given the preponderance of institutional path dependency in this policy sector, the affirmation of such long-standing partnerships and alliances should come as no surprise.

There are, however, two points with regard to multilateral organizations. First, although there are a number of persistent commonalities in memberships amongst the snapshots (e.g. EU, NATO) the states examined have different priorities of involvement, with some favoring one over the other depending on circumstances. For security purposes, the UK traditionally favors NATO with that organization's close relationship to the United States. The EU is seen as a socio-economic entity and national competences relating to security are strictly adhered to by the UK. Conversely, Germany and France are close partners with the EU. This is not to say that these two states value their membership of NATO less. Rather, that they have a wider conceptualization of security allowing them to perceive opportunities for the EU to provide some of that security and create European solutions which do not rely so heavily on the US. This is demonstrated by Finland; that country is a member the EU but not of NATO. Although Finland participates in NATO's Partnership for Peace it has chosen not to pursue full membership, but nevertheless is one of NATOs closest partners in cyberdefense. There are historical – i.e. path dependent – reasons for the differing prioritizations placed on international organizations. Since its inception, the EU has been regarded by its founding member states as not just an economic partnership, but a tool to promote security and reduce conflict in Europe.

The second point of note is more novel. There is a trend among the states examined to look further afield for actors with whom to cooperate and develop both economic and defensive alliances. Both France and the UK specifically mentioned BRICS and ASEAN member states as potential partners for international cybersecurity and cyberdefense cooperation. European countries casting their net of partnerships wider than their traditional spheres of influence may be innovative, but the partners they are targeting include some of the most digitally connected and advanced in the world. The level of penetration of digital and online technology in countries such as India, Japan and South Korea make them ideal partners for socio-economic and security cooperation. It should be pointed out, however, that Finland is something of an exception to this rule. Although it is a partner in cybersecurity and cyberdefense with the United States, it prioritizes its immediate neighbors in the Baltic and Nordic regions.

A second area of non-traditional partnerships occurs in relations with the private sector. All the states examined in this collection recognize the important role private sector entities play in holistic cyber security solutions, particularly given level of private ownership of the Internet and World Wide Web's infrastructure. Precise details of public-private partnerships (PPPs), however are scarce in the policy documents examined. Very little information is provided beyond historic service provision agreements, or the clarification that private companies are responsible for their own cybersecurity but that state authorities and services will provide support in the event of a major crisis. One noteworthy exception to this trend comes from the UK. The National Security Strategy explicitly states that national cyberdefense capabilities will be developed and operated by the private sector. On the face of things thins acknowledges where technical expertise and innovation resides. However, it sets a policy precedent, potentially opening the door for private sector entities to carry out cyberdefense operations. Responsibilities for ensuring the security of the state, a traditional responsibility of the national government, can potentially be outsourced to the private sector. As with other areas of cyberdefense however, precise details of this public-private relationship are not provided in the open-source policy documents.

7. Separation of cyberdefense from other national security/defense policies

One of the key idiosyncrasies identified when compiling the policy snapshots is the level of interconnectedness between cyberdefense policy and national security. In two cases cyberdefense is a separate policy area (France, Germany) with its own strategy or policy documentation. In other cases, such as the UK and Finland, cyberdefense is folded into wider national security frameworks without a separate strategy. This is not to say that they will not be separated at some point in the future, however current policy indicates it is to be better integrated into wider national security and defense considerations.

At first glance, this difference in document production could be interpreted as meaning that cyberdefense is given *greater* prioritization in those states where it is given its own documentation. However, the difference relates less to respective prioritization than to differences in historical and institutional cyberdefense policy development. The UK, for instance, has followed the American example and historically folded cyberdefense into its national security strategy. This demonstrates once again that path dependency plays a greater role in national policy development than differences in prioritization, in a similar manner to the tenor of the overall development of cybersecurity and cyberdefense policy in general.

8. Role – or absence – of the intelligence community in cybersecurity and cyberdefense

A final point to make is the lack of explicit information regarding the role in cybersecurity and cyberdefense of the intelligence agencies of each state. A dearth of detail regarding specific operational activities or capabilities is not unexpected given the sensitive nature of such activities; states will naturally be reluctant to place classified details in

the public domain. The policies examined provide some information regarding the position of intelligence agencies within national operational frameworks and structures and their relationship with other agencies in the wider cybersecurity and cyberdefense context. In the majority of cases this position is one which demonstrates a high level of civilian oversight of intelligence activities. However, this is where the exposition ends; there is very little attention paid to the involvement of intelligence agencies in policy development or the kind of advice or information, if any, that these agencies provide to that process. The ongoing exercise of developing and updating the national snapshots will highlight whether this is a trend, or whether the increased national scrutiny of the activities of intelligence agencies will give greater policy transparency in this regard.

9. Conclusion

The examination in this collection of four important European actors has yielded important findings, not least that precise policy and clear definitions in this field remains vague, and that there is a trend towards centralizing oversight and implementation responsibility for cybersecurity and cyberdefense. This centralization reflects the fact that cybersecurity issues are not restricted to one area of policy. As more and more devices become connected to the Internet, and as more and more social and infrastructure systems utilize those connected devices, the risks to national resilience and security have spread throughout all national policy areas, from defense and healthcare to banking and energy production. State authorities have recognized this trend and are acting accordingly. However, further research is needed to determine the extent of this centralizing trend. This collection is intended as a starting point for this continuing research.

The snapshots contained here are therefore the commencement of a larger research project intended to set out the state-of-play of national cybersecurity and cyberdefense policy around the world. Successive editions will add further snapshots as well as regional classifications, which will enhance our knowledge and understanding of policy in this field. This collection is the first step in this project. Furthermore, the analyses presented here should be considered “living documents”. As state priorities, governments and policy documents change or are reviewed, and as the cybersecurity and cyberdefense sectors continue to develop, the analyses themselves will be reviewed and supplemented to reflect any changes. This way, the collection will provide, and continue to provide, an up-to-date understanding of policy in an important global security field.

Contributors

Marie Baezner
Marie Baezner is a Researcher in the Cyber Defense Team of the Center for Security Studies, ETH Zurich. She holds a MA in International Security from the University of Bath, United Kingdom and a BA in International Relations (Political Science and International Law) from the University of Geneva. Before joining the CSS Marie Baezner has worked for the Command Support Basis of the Swiss Armed Forces and for the Swiss Armed Forces Peace Support Mission in Kosovo. Marie's research focuses on cyber-incidents and cyber aspects in current conflicts.

Sean Cordey
Sean is a former summer intern in the Cyber Defense Project at the Center for Security Studies, ETH Zurich. He holds a Bachelor of Arts in International Affairs from the University of St. Gallen. His BA thesis was a comparative policy analysis of the cybersecurity strategies of Switzerland, Austria and Germany.

Dr. Robert S. Dewar
Robert Dewar is a Senior Researcher in the Cyber Defense Team of the Center for Security Studies, ETH Zurich. He holds a PhD in Politics and an MSc in Global Security (Politics, Information and Security) from the University of Glasgow, and an MA (Hons.) in Modern History from the University of St Andrews. His PhD thesis was an examination of institutional dynamics in EU cyber security policy-making. Robert's research interests cover cyber security and defense policy, security studies, the European Union and historical institutionalism. Before joining the CSS Robert was a lecturer and tutor at the University of Glasgow and the University of Stirling. He taught courses on international relations, cyber security and the European Union.

Patrice Robin
Patrice is a former Project Assistant in the Cyber Defense Project at the Center for Security Studies, ETH Zurich. He holds a Master of Arts in Comparative and International Studies from the Swiss Federal Institute of Technology in Zurich and a Bachelor of Arts in Political Science from the University of Zurich. His MA thesis analyzed the impact of the Convention on Cybercrime on the number of convicted cyber criminals.

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.