NATIONAL CYBERSECURITY AND CYBERDEFENSE POLICY SNAPSHOTS

Updated Collection 2

Edited by Sean Cordey and Robert S. Dewar

Zürich, September 2019

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

Editors: Sean Cordey and Robert S. Dewar

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

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

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

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

Please cite as: Sean Cordey and Robert S. Dewar, ed. (2019): National Cybersecurity and Cyberdefense Policy Snapshots: Updated Collection 2, 2019, Center for Security Studies (CSS), ETH Zürich.

Contents

Introduction

Robert S. Dewar
Center for Security Studies, ETH Zürich[1]

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 cyber-conflict 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. Cyber-conflict 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 baseline 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.[2] 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 2019 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 eight important European and international actors – Austria, Finland, France, Germany, Italy, the Netherlands, the United Kingdom and Singapore. 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.

[1] Robert S. Dewar is now Head of Cyber Security at the Geneva Centre for Security Policy.

[2] 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.

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)[3] and NATO's Cooperative Cyber Defense Centre of Excellence (CCDCOE).[4] 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 cybersecurity or cyberdefense 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 or based on the ones in the national policy documents themselves. 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

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

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

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 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.

Austria

Sean Cordey
Center for Security Studies
ETH Zürich

Highlights/Summary:

1. Key national trends

Austria is a proactive European and international actor in the field of ICT and makes extensive use of its soft power, neutrality and diplomatic capital to promote an open and secure cyberspace. The current deterioration of the security situation in Europe and a growing sense of insecurity at the national level have led to a consolidation of Austria's cyberarchitecture and an intensification of the country's international engagements and cooperation, most notably with NATO, the OSCE and the EU.

2. Key policy principles

2.1 Cybersecurity

The Austrian approach to cybersecurity is inherently holistic and comprehensive and focuses on strengthening the resilience of critical infrastructure, capacity building (civil and military, state and private), cybercrime prevention, international cooperation, awareness-raising and the integration of all key players in the domains of cybersecurity and cyberdefense. Overall, Austria is currently in a phase of consolidating its cybersecurity and cyberdefense sectors.

2.2 Cyberdefense

There is no independent public cyberdefense policy or strategy in Austria. However, the tasks, objectives and role of the military in terms of cyberdefense are addressed in the cybersecurity strategy and the 2015 Military Strategic Concept. Furthermore, military cyber forces with offensive capacities have been established (BMLVS, 2015, p. 52).

3. Key national framework

3.1 Cybersecurity

Austria's cybersecurity policy is, at the strategic level, led by civilian authorities, namely the centralized Cybersecurity Steering Group (CSS) under the aegis of the Federal Chancellery (BKA), and it is informed by the Cybersecurity Platform (CSP), a Public-Private Partnership (PPP). At the operational level it is led by the Federal Ministry of the Interior (BM.I) and Federal Ministry of Defense (BMLVS) through their respective Cybersecurity and Cyberdefense centers, which form part of the inner circle of the operational coordination structure (IDOK).

3.2 Cyberdefense

The Federal Armed Forces (ÖBH) are integrated into the comprehensive provision of cybersecurity by the state. As such, they are primarily responsible for cyberdefense, which encompasses the protection of Austria's sovereignty in cyberspace, the protection against external threats, the protection of their own networks, the development of expertise, and support for the protection of critical infrastructures.

4. Level of partnership and resources

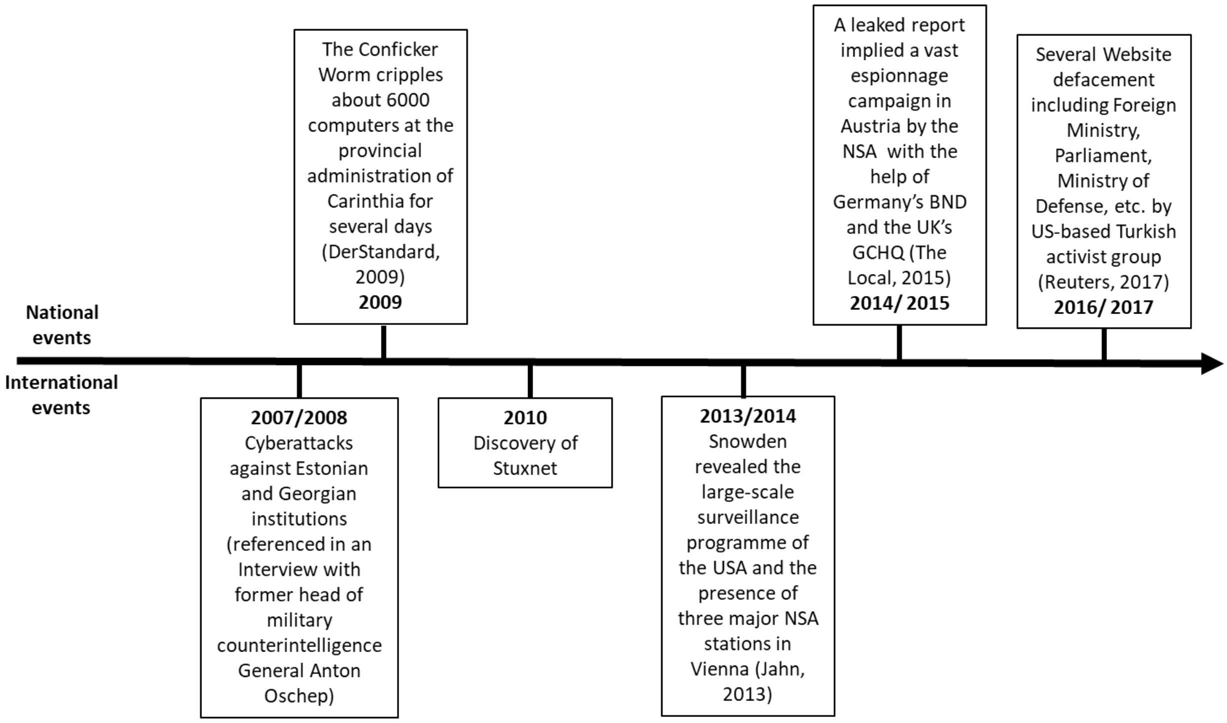
Austria's key regional and international partners are the European Union (including the European Defence Agency, the European Network and Information Security Agency and Europol) and – despite not being a member – NATO (through the country's participation in the Cooperative Cyber Defence Centre of Excellence and cyberdefense exercises). Austria also pursues bilateral cyber cooperation with Israel and Russia as well as its central European neighbors within the framework of the Visegrad group.

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

1.1 Threat perception: trigger events

Austrian policy documents relating to cybersecurity and cyberdefense do not refer to specific events. The following list of events, while not exhaustive, is based on news reports and information gleaned from interviews with public authorities:

Diagram AT1: Timeline of trigger events



National events

The Conficker Worm cripples about 6000 computers at the provincial administration of Carinthia for several days (DerStandard, 2009) **2009**

A leaked report implied a vast espionnage campaign in Austria by the NSA with the help of Germany's BND and the UK's GCHQ (The Local, 2015) **2014/ 2015**

Several Website defacement including Foreign Ministry, Parliament, Ministry of Defense, etc. by US-based Turkish activist group (Reuters, 2017) **2016/ 2017**

International events

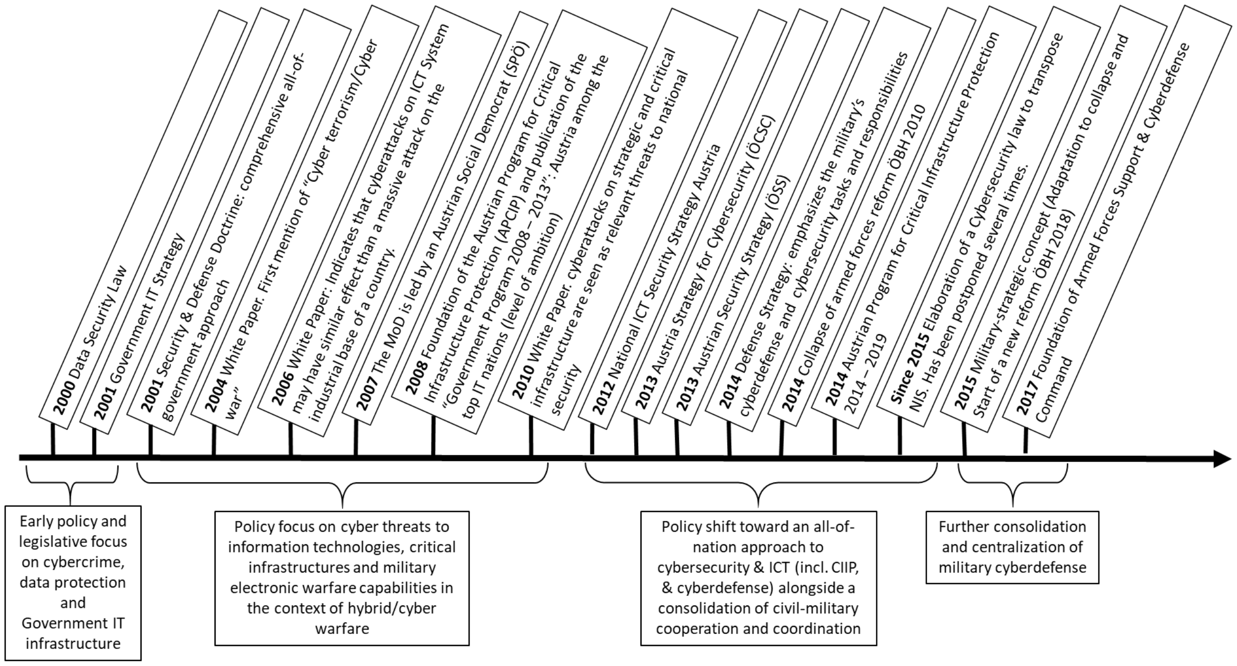
2007/2008 Cyberattacks against Estonian and Georgian institutions (referenced in an Interview with former head of military counterintelligence General Anton Oschep)

2010 Discovery of Stuxnet

2013/2014 Snowden revealed the large-scale surveillance programme of the USA and the presence of three major NSA stations in Vienna (Jahn, 2013)

1.2 Main policy documents: key shifts in strategy

Diagram AT2: Timeline of policy developments and trends



2000 Data Security Law

2001 Government IT Strategy

2001 Security & Defense Doctrine: comprehensive all-of-government approach

2004 White Paper. First mention of "Cyber terrorism/Cyber war"

2006 White Paper: Indicates that cyberattacks on ICT System may have similar effect than a massive attack on the industrial base of a country.

2007 The MoD is led by an Austrian Social Democrat (SPÖ)

2008 Foundation of the Austrian Program for Critical Infrastructure Protection (APCIP) and publication of the "Government Program 2008 – 2013": Austria among the top IT nations (level of ambition)

2010 White Paper. cyberattacks on strategic and critical infrastructure are seen as relevant threats to national security

2012 National ICT Security Strategy Austria

2013 Austria Strategy for Cybersecurity (ÖCSC)

2013 Austrian Security Strategy (ÖSS)

2014 Defense Strategy: emphasizes the military's cyberdefense and cybersecurity tasks and responsibilities

2014 Collapse of armed forces reform ÖBH 2010

2014 Austrian Program for Critical Infrastructure Protection 2014 – 2019

Since 2015 Elaboration of a Cybersecurity law to transpose NIS. Has been postponed several times.

2015 Military-strategic concept (Adaptation to collapse and Start of a new reform ÖBH 2018)

2017 Foundation of Armed Forces Support & Cyberdefense Command

Early policy and legislative focus on cybercrime, data protection and Government IT infrastructure

Policy focus on cyber threats to information technologies, critical infrastructures and military electronic warfare capabilities in the context of hybrid/cyber warfare

Policy shift toward an all-of-nation approach to cybersecurity & ICT (incl. CIIP, & cyberdefense) alongside a consolidation of civil-military cooperation and coordination

Further consolidation and centralization of military cyberdefense

1.3 Organizational structures: key parameters

In terms of cybersecurity and cyberdefense, Austria has adopted a holistic approach which is focused on the security and resilience of infrastructure and services in cyberspace as well as awareness and confidence building throughout Austrian society (BKA, 2013, p. 4). Consequently, and in view of Austria's decentralized, federalist system, the various policy areas are not centrally managed, and no national government agency has a monopoly on cybersecurity or cyberdefense policy. As a result, a number of different agencies have accumulated tasks relating to these areas, and a Cybersecurity Steering Group (CSS[5]) was established under the auspices of the Federal Chancellery (BKA[6]) to increase cooperation and coordination between these bodies. This group has the overall strategic leadership in cybersecurity and cyberdefense policy-making. It provides the overarching policy development and coordination and is supported by the Cybersecurity Platform (CSP), a public-private partnership (PPP).

In terms of policy operationalization, two ministries lead the policy process, namely the Federal Ministry of the Interior (BM.I[7]) for cybersecurity and the Federal Ministry of Defense and Sports (BMLVS[8]) for cyberdefense. Both ministries have set up dedicated bodies, namely the Cybersecurity Center (CSC) and the Cyberdefense Center (CDC) respectively. These two centers, along with several other bodies detailed in part 3.2, are part of the Inner Circle of the Operational Coordination Structure (IKDOK[9]), which is responsible for overall crisis management, operational implementation and situational assessment. In the context of national defense, the Austrian Armed Forces (ÖBH[10]) under the leadership of the BMLVS, are responsible for security in cyberspace as well as for the security of their own digital networks.

Overall, the supervision and coordination of cybersecurity falls within the responsibility of civilian authorities during peacetime, in particular the Federal Chancellery, but with the involvement of the military at all levels (e.g. in the CSS). Nonetheless, the general process remains highly collaborative and consensual, aimed at bringing together all of the parties involved in the civilian, military and private sectors.

1.4 Context/analysis: key national trends

The Federal Republic of Austria is a parliamentary democracy which has maintained, since its foundation, a policy and tradition of active neutrality as well as humanitarian action. Situated at the geographical heart of Europe, Austria is a proactive international player that makes extensive use of its soft power and diplomatic capital, for instance by hosting numerous international talks. Furthermore, thanks to Austria's enduring post-war legacy of neutrality, Vienna has become home to more than 100 international organizations covering a wide range of areas, among them the IAEA, OSCE, OPEC, UNICEF and UNHCR.[11]

Austria is also a proactive player in regional and European affairs as a member of the EU. Being one of the smallest member states in the Union and a non-NATO member, it holds a somewhat unique position, which has notably materialized in the country's active role in "bridge-building to the east", where Austria promotes stronger contact with Eastern Europe and the states of the former Soviet Union at all levels and supports EU membership of Balkan countries. Austria, however, is not a member of the Visegrad group[12], which is concerned with cooperation between other Central European EU members. In recent years, other policy areas of interest for Austria have included environmental policy, the common security and defense policy, cybersecurity (e.g. during its shared presidency with Estonia and Bulgaria) and, since the last elections, immigration policy. The latter must be considered within the context of the immigration crisis in Europe and the formation of a governing coalition between the populist right-wing Austrian People's Party (ÖVP) and the far-right Freedom Party of Austria (FPÖ).

In terms of security perception, Austria has become particularly concerned with the increasing deterioration of the security situation in eastern and southern Europe as well as the emergence and intensification of new security threats in general (i.e. border security, hybrid threats and terrorism) but also specific cyberthreats (i.e. cybercrime, cyberespionage, patriotic hackers, electoral cybersecurity).

[5] Cyber Sicherheit Steuerungsgruppe

[6] Bundeskanzlerei

[7] Bundesministerium für Inneres

[8] Bundesministerium für Landesverteidigung und Sport

[9] Innerer Kreis der Operativen Koordinierungsstrukturen

[10] Österreichisches Bundesheer

[11] For a full list please see https://www.austria.org/international-organizations/

[12] Composed of Poland, Czech Republic, Hungary and Slovakia

At the national level, this increasing insecurity perception has been accompanied by a long-standing reconsideration of the role and organization of the Austrian Armed Forces (ÖBH). However, relevant efforts stalled after long-planned army reform failed in 2014 due to political resistance and a lack of financial and human resources (BMLVS, 2015, p. 7). Nonetheless, Austria is currently making a new attempt to reform its armed forces. Military spending has increased as a result, from 0.55% of GDP in 2016 to 0.58% in 2018 (ORF news, 2018).

At the international level, this has led to a gradual strengthening of Austria's international security engagement (including cyberdefense) and cooperation. For example, while Austria is not a NATO member, it closely cooperates with NATO on education, training and the development of military capabilities through its Partnership for Peace (PfP). It also regularly attends and participates in NATO's Cyber Defense Committee and the CCDCOE (Cyber Sicherheit Steuerungsgruppe, 2018, p. 21). Furthermore, due to Austria's dual membership in the EU and UN and active engagement in strategic culture, the country's armed forces have participated in numerous peacekeeping operations and missions under the aegis of the UN, EU and NATO (e.g. Afghanistan, Kosovo, Bosnia and Herzegovina).

In terms of economic performance, Austria ranks among the world's 14 most prosperous countries, having a GDP per capita similar to that of Germany or Sweden (International Monetary Fund, 2018). While its ICT industry is not among the most developed or mature – it ranks 20th in the World Economic Forum's Networked Readiness Index (2016), and the Austrian government has made increasing efforts to harness the economic and social benefits of digital technologies, while mitigating their risks and associated impacts. In this context, Austria has been very active in trying to instigate a cybersecurity culture while promoting and securing the digital society and economy. As such, the protection of information, its systems and other digital assets as well as the development of expertise have been seen as key to guaranteeing the development of Austria's business environment and supporting the national economic and social model.

2. Current cybersecurity policy

2.1 Overview of key policy documents

Austria's security and cybersecurity policy have been devised in several policy documents that are introduced in the following paragraphs. These, in turn, are all deeply interconnected and integrated to form a comprehensive security policy under the umbrella of the Austrian Security Strategy. They are supplemented by a number of sub-strategies and departmental policy documents, such as the BMLVS' regular white papers and the Austrian Cybersecurity Strategy. It must, however, be noted that no specific cyberdefense strategy has been published.

2.1.1 Austrian Security Strategy 2013

Austrian security policy is based on the concept of "comprehensive security provision", in which the different policy areas work together on the basis of the overall Austrian Security Strategy (ÖSS[13]). The ÖSS thus serves as the overarching framework document for security policy in Austria, from which all sub-strategies are derived (defense policy, home affairs, cybersecurity, etc.). The strategy also mentions the EU as the central framework for Austrian security policy (BKA, 2013, p. 12).

The cyber domain encompasses aspects of internal security (cybercrime) as well as defense policy (military defense in cyberspace). Of particular note is the fact that the ÖSS underlines that cyberattacks are a military issue (BKA, 2013, p. 11). In addition to its conceptual part, the strategy also contains a section outlining the design principles for Austrian security policy (BKA, 2013, p. 17), which provide for the following basic measures and guidelines in the cyber domain:

1. General recommendations
    a. Strengthened security of computer systems and the Internet
    b. Implementation and development-driven updates of the Austrian Cybersecurity Strategy
2. Internal security
    a. Establishment of a competence center on cybercrime
    b. Active shaping of EU policy to protect citizens and businesses in cyberspace
3. Defense policy
    a. Special attention to cybersecurity in military training
4. Military national defense
    a. Protection of military installations against cyberthreats
    b. Integration of military capabilities with the national cyber concept
5. Assistance tasks and military disaster relief
    a. Critical infrastructure protection, including capacity-building and cybersecurity expertise
    b. Improvement of the military's cyberspace protection capabilities

2.1.2 National ICT Security Strategy Austria 2012

The National ICT Security Strategy Austria, published in 2012, is a comprehensive strategy that sets out guidelines and serves as a basis for the Austrian Cybersecurity Strategy (ÖSCS). As such, it seeks to address the growing disparities between actual ICT usage, increasing IT crime, necessary IT knowledge and risk awareness through a holistic, bottom-up approach (Digital Austria, 2012, p. 4). In order to do so, the strategy establishes an overarching framework and sets out principles, objectives and measures for ICT security in particular and cyberspace security in general (Digital Austria, 2012, p. 4). The strategy's main measures are as follows (quoted verbatim):

1. Stakeholders and structures
    1. Optimizing the cyber landscape in Austria
        i. Creation of a cyber-partnership (i.e. CSP, CSK)
        ii. Creation of a Cyber Situation Center[14]
    2. Establishing networks between stakeholders and structures
    3. Enhancing the legal framework for cybersecurity in Austria
    4. Promoting international cooperation

[13] Österreichische Sicherheitsstrategie

[14] Its intended tasks were ultimately divided between the GovCERT, the CSC and CDC.

2. Critical infrastructures
    1. Improving cyber crisis management
    2. Enhancing risk management and information security
    3. Information exchange between public and private stakeholders
3. Risk management and status quo
    1. Identifying core enterprises in the respective sectors
    2. Comprehensive risk and security management across sectors
    3. Ensuring minimum standards and managing risk acceptance in core enterprises
    4. Establishing crisis and emergency management in ICT and non-ICT sectors
    5. Assessment and management of the situation
4. Education and research
    1. Education/training relating to ICT, ICT security and media skills in early grades at school
    2. Compulsory ICT training for all students of teacher training programs
    3. Increased training of ICT security specialists in the tertiary sector
    4. ICT security as an important element of adult education and training
    5. ICT security research as a basis for national competence
    6. Increased coverage of ICT security topics in applied ICT research
    7. Active theme leadership in international research programs
5. Awareness
    1. Strengthening Austria's ICT security culture
    2. Positive positioning of ICT security
    3. Harmonized and coordinated approach
    4. Effectiveness and sustainability of awareness measures

2.1.3 Austrian Cybersecurity Strategy 2013

The Austrian Cybersecurity Strategy (ÖSCS[15]), published in 2013, was the first strategy in this field. Existing strategic and military documents are summarized in 2.3 below to provide an overview of existing cyberdefense efforts.

The ÖCSC is embedded in the overall Austrian security policy and was developed on the basis of the ÖSS while respecting the framework and principles set out by the Austrian program for the protection of critical infrastructures. As such, it can be understood as a kind of sub-strategy within Austrian security policy. In terms of content, the strategy provides the conceptual framework and describes the Austrian understanding of cybersecurity policy, the principles according to which it is designed, the political fields of action and the associated measures. These are elaborated in more detail in the following section.

2.2 National cybersecurity strategy: fields, tasks, priorities

Having mainly civilian character, the Austrian Cybersecurity Strategy 2013 presents itself as a comprehensive and proactive concept for protecting cyberspace and individual engagement with the virtual space[16] while guaranteeing human rights (BKA, 2013, p. 4). It lays down the core principles relating to cybersecurity policy, namely that it must be comprehensive, integrated and based on the principle of solidarity. In addition, it emphasizes that associated fundamental principles, such as the rule of law, subsidiarity, self-regulation and proportionality, and the general principles of ICT security also apply to cybersecurity.

Consequently, cybersecurity is understood as a central joint challenge for the state, economy and society, and cyberspace is conceptualized as a vital multidimensional space of action (information and communication space, social interaction space, economic and commercial space, political participation space, control room) for the state, business, science and industry. In particular, this space is about the protection of three elements, namely infrastructure, data and people, which are exposed to various risks and threats ranging from misuse to massive state-sponsored cyberattacks. Potential sources of threats include not only individual criminals and organized crime, but also foreign intelligence services and military forces.

The ÖSCS specifically states the following three overarching policy goals (BKA, 2013, p. 8):

[15] Österreichische Strategie für Cyber Sicherheit

[16] Used synonymously to Cyberspace in the policy documents

- To help shape cyberspace in a positive way in the interest of citizens, academia and the state;
- To prevent threats to cyberspace and the people in cyberspace from emerging or becoming effective ("prevention");
- To protect the legal asset of "cybersecurity" against threats as well as to cope with them.

Furthermore, the ÖSCS formulates the following nine strategic goals (BKA, 2013, p. 9):

1. A secure, resilient and reliable virtual space;
2. Secure and resilient state ICT infrastructures based on a national approach;
3. Protection of cybersecurity as a legal asset;
4. Creation of a "culture of cybersecurity" through awareness-building;
5. Positioning of Austria as a "pioneer in implementing measures to secure the digital society";
6. Active participation in international cybersecurity cooperation (e.g. international strategies);
7. Secure e-government of the Austrian administration;
8. Protection of own applications, customer identities and privacy by Austrian companies;
9. Assumption of individual responsibility in cyberspace by the Austrian people.

In terms of specific measures, the focus is mainly on establishing (or reinforcing) the national cybersecurity architecture and processes, including the cybersecurity steering group, operational-level coordination, cyber crisis management, the cybercrime center, GovCert and MilCERT; defining and clarifying the governance structure and the roles and responsibilities of the different actors; strengthening cooperation between the economy, government and society, notably through a cybersecurity platform (i.e. a PPP), awareness-building programs for SMEs and a Cybersecurity Communication strategy[17]; improving critical infrastructure protection; strengthening cybersecurity awareness and education; promoting R&D; and, finally, pursuing regional and international cooperation.

2.3 National cyberdefense strategy: fields, tasks, priorities

From 2004 to 2012, the BMLVS published a number of white papers. These comprehensively discuss and describe Austria's security policy principles, challenges, risks and international cooperation as well as planning and mandates for the armed forces, R&D, education and a long-term vision. Among these, the white papers have – since at least 2004 – touched upon various cybersecurity and cyberdefense-related matters. In the 2010 white paper, cyberattacks against strategic and critical infrastructures are elevated to national security threats. While the initial focus was on "cyberterrorism", it has since shifted towards issues pertaining to cyberwar, critical infrastructure protection (CIP), international cooperation and the ÖBH's contribution to state security (BMLVS, 2013). For example, the 2006 White Paper was the first to note that cyberattacks on a country's ICT systems could have a similar impact as serious attacks on a country's industrial base.

Meanwhile, Austria has no specific cyberdefense strategy per se, however, the most recent installment (2015) of the Military Strategic Concept (MSK[18]) describes the underlying field, tasks and priorities of the Austrian armed forces in this domain. Broadly, the MSK focuses on ensuring the military-strategic implementation of the Austrian Security Strategy and the defense policy sub-strategy 2014 (TV[19]); creating the conceptual basis for the implementation of the reform of the Austrian armed forces (ÖBH 2018); preparing the ÖBH at home and abroad; further developing non-conventional national defense, including cyberdefense; teaching and R&D; and, finally, the overall military development in Austria. Compared to the previous strategic concept from 2006, the MSK 2015 focuses particularly on cyberdefense, cyberthreats (risks, dependencies, etc.) as well as different tasks and capabilities, based on a description of different scenarios.

In particular, it provides a number of guidelines and measures specific to cyberdefense. As such, it underscores the continuing need for military capabilities to provide comprehensive domestic security against new, non-conventional risks and to contribute to international crisis management. The national defense in cyberspace will be expanded further for this purpose.

The MSK 2015 also defines the tasks, mandate and associated ambition of the ÖBH in term of cybersecurity and cyberdefense and is the only document that deals with both offensive and defensive cyber procedures. The main tasks of the military are thus threefold: cyberdefense, comprising operations in the cyberspace and the defense against cyberattacks on Austria's sovereignty; protection of military infrastructures, networks and personnel as well as protection of constitutional institutions, the population and their livelihoods; and cyber deterrence. Furthermore, the

[17] Which was developed by 2015 but has not yet been publicly released

[18] Militärstrategisches Konzept

[19] Teilstrategie Verteidigungpolitik 2014

armed forces also support civilian authorities in terms of critical infrastructure protection, cyber crisis management, cybersecurity awareness and European cyberdefense in general.

Furthermore, in order to build up a permanent military defense in cyberspace, the MSK 2015 calls for the so-called "cyber forces" to be assigned to the combat troops and to employ both defensive and offensive operations to fulfill their mission (BMLVS, 2015, p. 52) in case of a large-scale cyberattack against Austrian institutions and critical infrastructures.

2.4 Context/analysis: key policy principles

In times of peace, Austria's cybersecurity policy is steered, owned, coordinated and led by civilian authorities, namely by the government and Chancellery through the Cybersecurity Steering Group. This Group is supported and advised by private, public, societal and academic stakeholders via the Cybersecurity Platform, a PPP. Operational authority and responsibility is divided between multiple bodies and ministries, the most senior of which are the Ministry of the Interior (BM.I) for all matters concerning cybersecurity at large, and the Ministry of Defense (BMLVS) for all matters related to cyberdefense. Furthermore, Austria has also set up a unique operational coordination structure which is divided into an inner and an outer circle to integrate all relevant stakeholders within the public and private spheres.

At the national level, Austria's cybersecurity policy is closely integrated with its national security policy, strategy and framework. As such, it is a sub-strategy developed on the basis of not only the Austrian Security Strategy (ÖSS) but also some of its other (sub-)strategies such as the ICT Security Strategy Austria and the Austrian Program for Critical Infrastructure Protection (APCIP). Furthermore, Austria explicitly follows a proactive, comprehensive all-of-society security approach, which closely interlinks both external and internal security as well as civilian and military security. This is underlined by a robust collaborative model that encompasses and recognizes the roles and responsibilities of all relevant stakeholders at all levels of government. It also emphasizes task-sharing between the state, business, academia and civil society. This is notably demonstrated by the dual chairmanship of the CSS by the heads of the cybersecurity and cyberdefense centers and the inclusion of representatives of provincial governments. Interestingly, but not surprisingly considering its humanitarian tradition, Austrian policy documents emphasize a solidarity-based cybersecurity policy at the European and international level.

Austrian cybersecurity policy is based on two separate sets of driving principles, namely universal and fundamental principles. The former relate to the definition of Austria's ICT security strategy in general terms: confidentiality, integrity, mandatory application, authenticity, availability as well as privacy and data protection. The latter include not only the rule of law (i.e. compliance with human rights) and subsidiarity (cf. federalism) but also the principles of self-regulation (notably in the private sphere[20]) and proportionality (BKA, 2013, pp. 7–8).

Cyberdefense policy is being developed as an integral component of the Austrian concept of "comprehensive security provision" and its associated cybersecurity frameworks. The military as a body is thus considered a key pillar of Austria's cybersecurity preparedness and resilience and operates closely alongside civilian cybersecurity bodies, which it supports. As such, the Austrian Armed Forces are primarily responsible for military self-protection, external security and the protection of the Republic's sovereignty in cyberspace. The Armed Forces' approach to cyber-operations – whether offensive of defensive – are only addressed in the MSK 15, albeit without further detail. However, the theorized use of defensive and offensive military cyber procedures as well as the creation and allocation of resources for military cyber forces (Cyber Sicherheit Steuerungsgruppe, 2015) causes Austria's implicit approach to be in conflict with the country's declared neutrality and position on the primacy of the state in defense matters.

While cybersecurity and cyberdefense have gained greater salience and priority in national policy since the end of the millennium's first decade, these domains are still not considered with the greatest urgency, as the migration crisis has taken precedence in Europe in recent years. Nonetheless, Austria has, under the guidance of the BKA and within the framework of the Austria ICT security strategy and the ÖCSC, consolidated its policies, structures – notably in terms of crisis management – and national and international initiatives since 2013. Together, these documents set out Austria's vision for cybersecurity, which focuses on ensuring a secure, resilient and reliable cyberspace and protecting users. In terms of results, the 2017 Global Cybersecurity index of the International Telecommunication Union (ITU) ranked Austria 30th – ahead of Italy and behind Uruguay – (ITU, 2017), thus identifying the country as being at a stage of maturation.

As mentioned above, Austrian policy documents in this domain focus on a range of measures to protect Austria's cybersecurity. These include *inter alia* the development of expertise, awareness-raising, and improved government information security infrastructures as well as increased international cooperation at the economic, diplomatic and

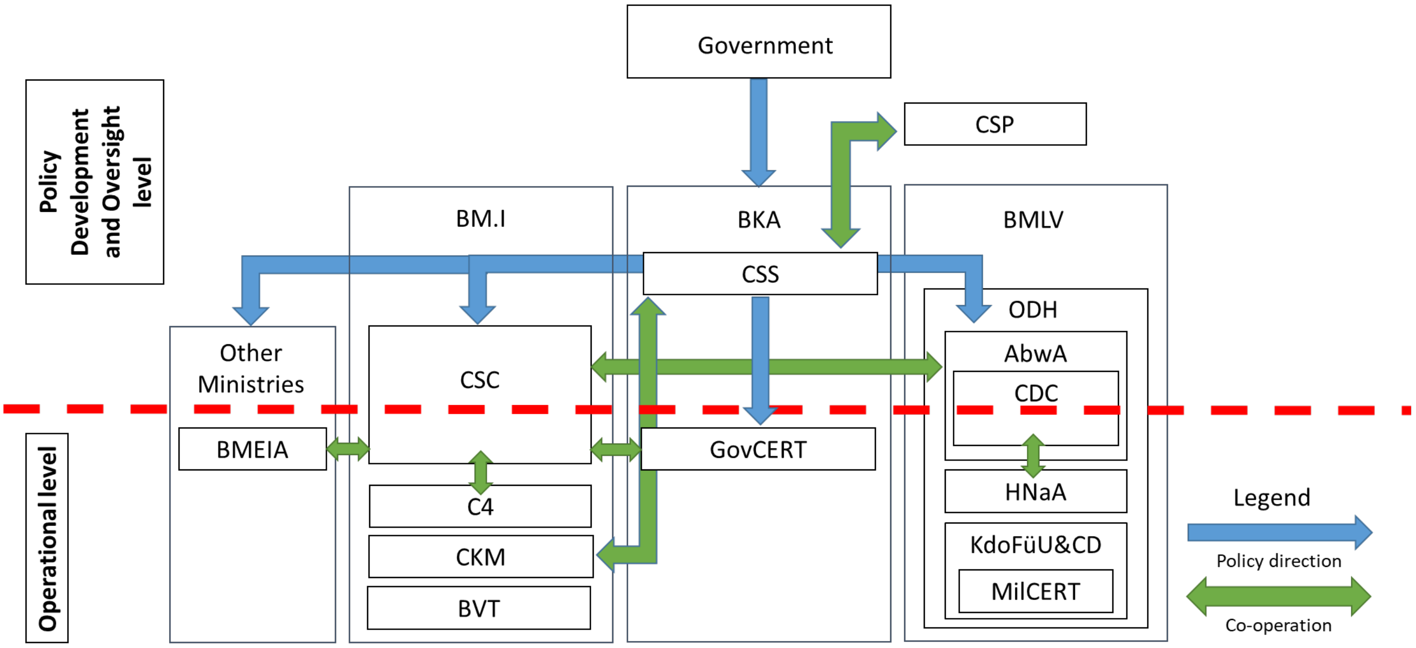
[20] "Self-commitment if possible, regulation if necessary"

military levels. As such, the scope is very comprehensive and similar to European counterparts as well as the European Union cybersecurity strategy, compared to international standards and policies.

3. Current public cybersecurity structures and initiatives

3.1 Overview of national organization framework

Diagram AT3: Oversight organization



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

3.2.1 The Inner Circle of the Operative Coordination Structure (IKDOK)

As prescribed by the ÖCSC, the Austrian Government established a "structure for coordination at the operational level" in 2016, which is tasked with periodic and case-related operational situation assessments for cybersecurity; the elaboration of measures in the event of an incident; and the support and coordination of national emergency measures within the framework of cyber crisis management (CKM) (Cyber Sicherheit Steuerungsgruppe, 2018, p. 31). This structure is composed of two overlapping "circles", namely the **Inner Circle (IKDOK[21])** and the outer circle. The former comprises the Cyber Security Center (CSC) and Cyber Defense Center (CDC), which jointly hold the chair; the Cyber Crime Competence Center (C4); the Army Intelligence Office (HNaA); Command Support and Cyber Defence with MilCERT (KdoFüU&CD); GovCERT; the Federal Ministry for Europe, Integration and Foreign Affairs (BMEIA); and the Office for the Protection of the Constitution and Counterterrorism (BVT). The latter is notably composed of CERT.at; EnergieCERT and other Sectoral CERTs (Cyber Sicherheit Steuerungsgruppe, 2018, p. 31). In case of a crisis, the IKDOK, supported by the outer circle actors, will form the nationwide Cyber Crisis Management (CKM), which is largely modelled after the state crisis and disaster protection management (SKKM[22]) system in terms of processes and mechanisms. Currently, it is in charge of the implementation of the EU NIS directive.

[22] Krisen- und Katastrophenmanagement

3.2.2 Cybersecurity Steering Group (CSS[23])

The **Cybersecurity Steering Group (CSS)** under the aegis of the Federal Chancellery is a statewide structure for cybersecurity coordination at the operational and political-strategic levels. Created in 2012[24], this body consists of liaison officers and cybersecurity experts of the National Security Council[25]**,** the Chief Information Officer of the Federal Republic of Austria and representatives of the competent ministries and Austrian federal provinces. In specific cases, it involves other representatives from industry and research. According to the ÖCSS, the CSS is tasked with coordinating cybersecurity measures, monitoring and supporting the implementation of the strategy, drafting annual cybersecurity reports (including threat analyses) and advising the government on cybersecurity matters.

3.2.3 Cyber-Crisis Management (CKM[26])

The **Cyber-Crisis Management** body provides a shared platform for all representatives of the state and operators of Austrian critical infrastructures in the event of a crisis. As such, its organizational, strategic and operational structure is modelled on and functionally integrated with the existing Government Crisis and Civil Protection Management (SKKM). The lead authority in terms of coordination regarding overarching threats is the BM.I, whereas the BMLV leads and coordinates measures to protect national sovereignty as far as external security is concerned. The CKM is tasked with developing continuity plans and exercises for the various entities, in addition to cyber crisis management.

3.2.4 Cybersecurity Platform (CSP[27])

The **Austrian Cybersecurity Platform (CSP)**, launched as a Public-Private Partnership (PPP) in March 2015, is the central information exchange and cooperation platform for all cybersecurity stakeholders in Austria, whether from the business sector, academia, science or public administration. Chaired by the Federal Chancellery, it advises and supports the CSS on strategic cybersecurity issues and promotes the ongoing exchange of experiences and information in the cybersecurity domain with a particular focus on the operators of critical infrastructures in order to strengthen their resilience. Together with the CSS, the platform has also launched an extensive program relating to awareness-raising (notably targeted at SMEs and coordinated by the Federal Ministry for Digital and Economic Affairs) and training as well as a research and development initiative. It additionally acts as the umbrella organization for existing cooperation formats, such as the Board of Trustees Secure Austria, Austrian Trust Circle, Cyber Security Forum, Center for Secure Information Technology - Austria, Cyber Security Austria, CERT-Verbund) (Digital Oesterreich, n.d.).

In terms of organization, the CSP is composed of the plenum, a number of working groups (AG) and the secretariat. It meets once or twice a year in plenary sessions, which are attended by stakeholders from public administration, business, science and research as well as representatives of private cybersecurity initiatives. The workings groups, which form the operational arm of the CSP, comprise topic-related, industry-related and organization-related groups. A specific working group for the Cyber Security Agenda 2020 was set up as part of the platform, which is tasked with reviewing and contributing to the further development of the second iteration of the cybersecurity strategy. Finally, the secretariat supports all activities of the plenum and the working groups. The secretariat is hosted by the Federal Chancellery and supported by the BM.I and BMLV, if necessary (Digital Oesterreich, n.d.).

3.2.5 Cybersecurity Center (CSC)

The **Cybersecurity Center (CSC)** was established within the BM.I as a joint initiative with the EU[28] and input from the BVT. After 30 months of development and construction, the center was finally operational in December 2017. According to the latest (2018) cybersecurity report, the center's core tasks are as follows:

[23] Cyber Sicherheit Steuerungsgruppe.

[24] Following the decision of the Council of Ministers of 11th May 2012.

[25] The National Security Council is the central advisory body to the Federal Government in matters of foreign, security and defense policy. It is chaired by the Federal Chancellor and composed of representatives of the BMLVS, BMEIA, BKA, BM.I , BMVRDJ and political parties.

[26] Cyber Krisenmanagement

[27] Cyber Sicherheit Plattform

[28] The center was partly funded by the European Union's Internal Security Fund (ISF).

1. Role as the Network and Information Security (NIS) Authority
2. Prevention & protection of critical infrastructures (including awareness-raising and advisory workshops and presentations)
3. Coordination & cyber crisis management (including an early warning system)
4. Development and maintenance of technical competence (including cyberthreat analyses, a malware lab and an APT competence center)
5. Role as national and international liaison body

3.2.6 Cyber Crime Competence Center (C4)

The **Cyber Crime Competence Center (C4)**, established in 2012 within the BM.I, is the national and international cybercrime reporting and coordination unit. As such, it is staffed with specialized technology, criminal and forensic experts of the Federal Criminal Police Office (BK[29]), the Federal Office for the Protection of the Constitution and Counterterrorism (BVT[30]) and the Federal Anti-Corruption Bureau (BAK[31]) (Online Sicherheit.at, 2018). The C4 also acts as a point of contact for cybercrime issues for business, the administration and all police departments and provides assistance in securing electronic evidence (Cyber Sicherheit Steuerungsgruppe, 2017). The center's organization and technical development were completed in 2014 and its staff levels have been boosted over the years.

3.2.7. GovCERT

GovCERT is the national CERT for the public administration and critical infrastructures and performs both coordinating and operational tasks. It is Austria's cybersecurity point of contact and as such liaises with international organizations and CERTs. In addition, it pools security technology expertise and shares it with the public administration, including preventive measures, the collection and evaluation of security-related incidents and, if required, on-site support services. Other tasks include training programs, the coordination of theme-specific working groups, regular awareness-building measures, the further development of Austria's CERT system and participation in national and international cybersecurity exercises.

3.2.8 Federal Office for the Protection of the Constitution and Counterterrorism (BVT[32])

The **Office for the Protection of the Constitution and Counterterrorism (BVT)** is an Austrian police body under the jurisdiction of the BM.I that acts as the domestic intelligence agency. Its core mandate is to protect Austria's constitutional bodies and their ability to function. In addition, it is responsible for cooperation with foreign security authorities and intelligence services. In terms of cybersecurity, the official role and capabilities of the BVT are not publicly disclosed, neither in the ÖCSC nor in any other reports. Nonetheless, it actively participates in CSC tasks, notably in terms of cyberthreat analysis and risk assessment, which serves as an important decision-making basis for strategic management (Blauensteiner, n.d.; Cert.at, 2017).

3.2.9 Ancillary agencies

In addition to the dedicated cybersecurity agencies and bodies, there a several other federal government, semi-public and private entities which play a prominent role in Austrian cybersecurity. Of most relevance to the present analysis are:

- **CERT.at** is Austria's CERT, and its tasks are best described as those of an "Internet fire brigade". First and foremost, CERT.at becomes active whenever acute security threats arise based on internal investigations or observations and threat detection or after notification by affected bodies. As an information hub for cybersecurity issues, CERT.at is also a point of contact to which third parties may report acute security problems. Other responsibilities of CERT.at include preventive measures such as the early detection of threats, preparation for tackling incidents and cyberattacks, PR work and consultancy as well as networking with foreign CERTs.

[29] Bundeskriminalamt

[30] Bundesamt für Verfassungsschutz und Terrorismusbekämpfung

[31] Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung

[32] Bundesamt für Verfassungsschutz und Terrorismusbekämpfung

- The **CERT Alliance** was established in 2011 to support the collaboration between different Austrian CERTs and the public and private sectors. Its objective is to pool available resources and utilize joint expertise optimally to deliver maximum ICT security. The members of the Alliance are A1-CERT, ACOnet-CERT, BRZ CERT, CERT.at, GovCERT, milCERT, R-IT CERT and Vienna CERT.

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

The **Federal Ministry of Defense and Sport (BMLVS)** is the lead ministry with regard to cyberdefense matters. It is principally responsible for developing the capabilities necessary to defend Austria's sovereignty and to counter and deter possible cyberattacks. In addition, it is tasked with supporting the Ministry of the Interior with regard to operational coordination and situational awareness. The following agencies and entities are under its aegis:

3.3.1 Kommando Führungsunterstützung und Cyber Defence (KdoFüU&CD)

The **Command Leadership Support and Cyber Defense (KdoFüU&CD)** was established in January 2017 as part of the senior leadership of the Austrian Armed Forces. It is responsible for the overall internal coordination of the cyberdefense domain at the strategic, operational and tactical military levels (Cyber Sicherheit Steuerungsgruppe, 2018, p. 32). Accordingly, it brings together relevant skills in the areas of leadership support, ICT services, electronic warfare and operational cyberdefense, including education, training and professional development. Furthermore, it combines preventive, operational and reactive cyberthreat mitigation capabilities. In terms of military operations in cyberspace, the command closely cooperates with the Abwehramt (AbwA, Armed Forces Counterintelligence Service) and the Heeresnachrichtenamt (HnaA, Army Intelligence Office) (Cyber Sicherheit Steuerungsgruppe, 2018, p. 32).

Organizationally, a cyber-inspection and control (CIC) staff unit has been set up at the command level, which is further subdivided into the following six sections and two military units:

- ICT and Cyber Security Center (ZIKTCySih)
- Institute of Military Geosciences
- Applications area
- ICT technology sector
- ICT operation area
- Command Support School
- Command Support Battalion 1
- Command Support Battalion 2

In addition, the **Center for ICT and Cyber Security (ZIKTCySih)** was reorganized as an operational element in the wake of a massive expansion of its tasks. Specifically, the center is, in its role as **MilCERT**, responsible for the information and ICT security of all BMLV and ÖBH systems. The technical, tactical, strategic and organizational-procedural capabilities of cybersecurity and cyberdefense are concentrated within ZIKTCySih. Accordingly, it is also a member of the CERT network and contributes to the overall cyber crisis management of the national operational coordination structure (2018 report). Its key tasks are as follows (2014 report):

- To prepare periodic and incident-related operational cyber situation reports as well as to contribute to situation reports on cybersecurity
- To evaluate attack and defense technologies and to draft conceptual recommendations based on such evaluations
- To implement technical and organizational security checks
- To perform penetration testing and security audits of applications and systems
- To conduct static and dynamic code analyses during possible malicious code testing and to develop countermeasures
- To develop comprehensive security systems for networks, servers and user equipment
- To respond to and handle IT security incidents
- To observe and evaluate defense and attack technologies
- To develop and implement cyberdefense measures

3.3.2 Abwehramt (AbwA) – Cyberdefense Center (CDC[33])

The **Abwehramt (AbwA)** is one of the two military intelligence agencies of the Austrian Armed Forces. It is responsible for protecting the army itself and therefore implicitly also for detecting any deliberate attacks on military assets and resources (persons, property and secrets) that could impair Austrian military security and Austrian contingents deployed in missions abroad. As such, it operates the **Cyber Defense Center (CDC)**, which is responsible for collecting, aggregating, analyzing and disseminating broad situational information on cyberspace. This information in turn serves as the basis for the development of countermeasure options (Cyber Sicherheit Steuerungsgruppe, 2018) and supports the BMLVS and ÖBH in performing their national tasks of protecting sovereignty in the context of comprehensive national defense and security (Cyber Sicherheit Steuerungsgruppe, 2017). The CDC also acts as an operational NIS authority for matters falling within the remit of military national defense (Cyber Sicherheit Steuerungsgruppe, 2015, p. 30) and contributes to raising awareness of cybersecurity, notably through the organization of the yearly ICT Security Conference. Overall, the center will ultimately include 350 additional positions and attract an investment of €46 million for the purchase of hardware and software (Schmid, 2017).

3.3.3 Heeresnachrichtenamt (HNaA)

The **Army Intelligence Office** (Heeresnachrichtenamt/HNaA) is the second military intelligence agency of the Austrian Armed Forces. In terms of cybersecurity and cyberdefense, it is tasked with outlining the evolving strategic situation, especially with regard to international actors and developments. Its contribution then flows into a general comprehensive state situation analysis to serve as a possible basis for decision-making for the highest political and military leadership (Federal Chancellery of the Republic of Austria, 2014). Furthermore, the HNaA is responsible for the early detection of potential foreign cyberthreats as well as, in case of a large-scale cyberattack on national infrastructures, the identification of attackers.

3.4 Context: key public organizational framework

The Austrian cybersecurity organizational framework, which reflects the country's national security approach, is inherently holistic, integrated, multilevel and horizontal and emphasizes close inter-ministerial cooperation. More precisely, the political and strategic guidance and steering of cybersecurity and cyberdefense are centralized in the hands of the civilian federal government and the federal Chancellery, which hosts the CSS that devises strategic guidelines. The CSS in turn consults with the CSP, which brings together public and private stakeholders. The whole strategic process is also supported by hybrid strategic and operational bodies such as the CSC, CDC and CKM. At the same time, the operational development and day-to-day tasks are distributed between a number of stakeholders, whether governmental or private, (e.g. C4, HnAA, GovCERT, CERT.at, etc.), which are part of the inner or outer circle respectively. For those within the administration, most of these bodies are under the aegis of the two ministries which de facto lead the operational process and have the greatest powers and capabilities regarding implementation, namely the Ministry of the Interior and the Ministry of Defense. The role of the Ministry for Europe, Integration and Foreign Affairs and its representation tasks are nonetheless explicitly recognized – i.e. both in the ÖSCS and as part of the inner operational circle – but this ministry has not been allocated additional structures or bodies to perform this role. As such, the division of tasks between the two leading ministries (i.e. one each in charge of cybersecurity and cyberdefense) reflects the split of national security between internal and external security.

Overall, Austria has adopted a rather transformative approach creating most of its current cybersecurity architecture (apart from systems in place for cybercrime and its C4, which was an early focus) and bodies from scratch after the publication of its ICT security and cybersecurity strategies in 2012 and 2013 respectively. Setting up this architecture required not only considerable human, monetary and time resources, as is evident from the recent operationalization of the Cybersecurity Center (2017) and the Cyberdefense Center (2018), but also considerable effort in navigating associated bureaucratic and political complexities. Furthermore, due to the presence of a number of private and public associations and bodies (e.g. KSÖ, Cert.at) which had already acquired expertise and capabilities prior to 2013, the Austrian approach also entailed considerable consolidation, inclusion and a clear definition of tasks, resulting notably in the operational coordination structure of the outer circle. In this context, it is worth noting that Austria, perhaps unsurprisingly, relies on PPPs quite extensively to bring together all relevant stakeholders and address the needs of the various industries involved. One can assume that this operational structure works well for Austria,

[33] Cyber Defence Center / Cyber Verteidigungszentrum

given that there are relatively few actors (mainly due to the country's small size), a closely networked economy and elite, a tradition of strong public-private cooperation and a liberal policy of self-regulation and trust.

There are, however, some potential problems and shortcomings regarding this type of approach and architecture. For instance, there is a certain discrepancy in terms of the distribution of responsibilities between the civilian and military and the expertise of the various affiliated bodies. Without further, appropriate knowledge-building, this could lead to an unwanted dominance of one side or the other, which in turn could influence policy development in a biased manner. The most challenging issues are the remaining overlap of responsibilities, notably in terms of intelligence, which makes practical interdepartmental cooperation difficult; and the persistent competitive bureaucratic/political stance taken by the ministries involved, which leads to an inefficient use of resources. With regard to the former, this is especially prevalent between the BVT, CSC and HnaA and could present considerable challenges if there was a cyberattack similar to those committed against Austrian governmental institutions in 2017. Indeed, a differentiation between internal (purview of the civilian CSC and BVT) and external (purview of the army) security threats would be difficult and most likely cause both ministries to assume responsibility and take action in response. Accordingly, the fine line beyond which an event requires a military rather than a police response is difficult to define, especially given the current framework of hybrid warfare operations. These issues are interrelated in that the unclear separation of responsibilities among two ministries usually held by different political parties contributes to the creation of a climate of mistrust, competitive thinking and a certain degree of paranoia. This is exacerbated by the fact that the different ministries (mainly the BKA, BMLVS & BM.I) compete for future large-scale investments in cybersecurity, cyberdefense and cybercrime, which have been publicly announced but not yet disclosed in detail (Schmid, 2017). Additionally, they also compete in terms of experts and the development of competencies. Overall, this situation has prevented the formation of any clear and strong cyber leadership, which has not only hampered the implementation of the ÖSCS but also poses a critical problem should a large-scale cyberattack occur.

4. Cyberdefense and cybersecurity partnership structures and initiatives

4.1 Public-private cyberdefense partnerships

Since the early 2000s and the introduction of new public management, the Austrian government has frequently established public-private-partnerships (PPP) in various areas such as infrastructure construction, CIP and research and innovation. This is no different in the field of cybersecurity, but is not the case with cyberdefense, at least not in the public realm, as official documentation contains no references to specific PPPs with the military.

In terms of cybersecurity in general, the main PPP is the **Cyber Security Platform** (cf. 3.2.1), which brings together over a 100 stakeholders from business, science and administration. This platform delivers good practices for critical Infrastructure operators and acts as an information exchange and cooperation hub for these stakeholders (incl. the BMLVS). In addition, the CSP provides assistance in an advisory capacity to the CSS and acts as the umbrella for the following organizations:

The **Austrian Trust Circle (ATC)**, founded in 2010, is a joint initiative of CERT.at and the Federal Chancellery. Its primary goal is to foster trust and promote the exchange of information and experiences among key actors with regard to major strategic infrastructure sectors (CIIP) (Austrian Trust Circle, n.d.). It also sets up operational contacts and provides experts in the event of a crisis. Currently it addresses the energy, financial affairs, health, industry, transport and communication sectors. The ATC organizes quarterly sector-specific meetings and annual cross-sectoral conferences.

The **Secure Information Technology Austria Center (A-SIT)** is a non-profit association and competence center that supports the Austrian government in implementing effective laws on IT security. Its mission covers the sectors that are primarily concerned with information security, namely the public authorities, the financial community and the scientific community. It was established in 2000 by the Federal Ministry of Finance and the Austrian National Bank, and Graz University of Technology and the Federal Data Processing Center (BRZ) joined as members in 2012 (Graz University, n.d.).

The **Kuratorium Sicheres Österreich (KSÖ)**, founded in 1975 by representatives of the public sector, politics, business and academia, is a non-profit association that used to be part of the BM.I. It is concerned with business and state cooperation in the Austrian security domain. In terms of cybersecurity, the KSÖ has cooperated closely with the BM.I since the 2011 launch of the Cybersecurity Initiative and presents a cyber risk matrix for Austria on a regular basis. It additionally organizes the Austrian Cyber Security Challenge and the Cyber Security Conference (Kuratorium Sicheres Österreich, n.d.). In 2015, the KSÖ created the Cybersecurity Forum, which has since been rebranded as the Digital Security Platform and provides a forum for industry representatives (mainly operators of critical infrastructures) to meet and discuss best practices and challenges in the field of cybersecurity (ENISA, 2017, p. 28). At the international level, this body is a member of the **European Cybersecurity Organization** and its cybersecurity PPP, which has been working to develop a common approach and market for cybersecurity at the European level since 2016 and promotes the effective implementation of cross-sectoral regulatory requirements (European Cybersecurity Organisation, 2018).

Cyber Security Austria is another non-profit, independent and non-partisan association that addresses cross-cutting issues of IT and cybersecurity. As such, it promotes a holistic approach and awareness-raising both at all levels of society, extending from families to the media, NGOs, decision-makers, politicians, economic actors and academia, and in the context of specific critical information infrastructure such as in the chemical, energy, telecommunications, finance and health sectors, among others (Cyber Security Austria, n.d.). In addition, it proposes solutions and best practices for organizational and non-technical problems, supports crisis management at the national level and conducts vulnerability research.

4.2 International cyberdefense partnerships

Austria's international cyberdefense cooperation focuses on the regional level, namely frameworks of the EU, NATO and Visegrad Group. With regard to the EU, Austria cooperates with its European counterparts on issues of economic and industrial cybersecurity, cybercrime and cyberdefense. Specifically, it supports the work of the European Network and Information Security Agency (ENISA), the European law enforcement agency (Europol), the 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). Austria also participates in the EDA's Cyber Range Federation project alongside with ten other member states. This project aims to increase the availability of existing and emerging cyber range facilities; increase the occupation rate and efficiency of cyber ranges and platforms; and mainstream and improve cyberdefense training, exercises and testing at the European level (European Defence Agency, 2017). It therefore signed a Memorandum of Understanding (MoU) on the pooling and sharing of cyber range capabilities with Belgium, Estonia, Finland, Germany and Latvia in June 2018 (European Defence Agency, 2018). Lastly, Austria regularly takes part in various exercises organized at the European level such as EU CYBRID and EU PACE.

NATO is another of Austria's key cyberdefense partners, even though Austria is not a member of the alliance. Indeed, Austria has been, within the framework of NATO's Partnership for Peace (PfP), actively engaged in NATO's Science for Peace and Security (SPS) program, one of whose key priorities is cyberdefense (NATO, 2018). Austria participates in NATO's multinational R&D programs (e.g. NATO's CCDCOE), cyberdefense exercises (e.g. Lock Shields 17 & 18 and Trial Thor's Hammer II) and other capacity-building initiatives (e.g. the smart cyberdefense project) (2015 review report). In addition, Austria participates and engages in various cyberdefense-related meetings organized by NATO such as the C3 Board and the Cyberdefense Committee (i.e. 28+1 format in 2015) (Cyber Sicherheit Steuerungsgruppe, 2018).

Furthermore, despite not being a formal member of the Visegrad group, Austria also cooperates with this body in two contexts. The first is through the **Central European Cyber Security Platform**, launched in 2013, which serves as a common ground for sharing information and best practices and building capacity through joint exercises, trainings and research. The second is through its CERT and the CSIRT.SK (Kirňák, Šulc, Illési, & Gapiński, 2016).

Austria also holds bilateral consultations on various cybersecurity-related issues with Russia and Israel (Cyber Sicherheit Steuerungsgruppe, 2018). In addition, the BKA and its Swedish counterpart have established an annual Austrian-Swedish Cyber Security Program, which links leading Swedish and Austrian operators of CI in telecommunications, finance, energy and transportation with selected providers of state-of-the-art technology to develop solutions for future cybersecurity needs (Cyberwiser, n.d.).

Austria first participated in these consultations in 2017. This engagement has provided a forum in which experience required for the continued protection of the Austrian Federal Armed Forces could be developed under real conditions so that the country will be better able to protect its soldiers during future missions. This multinational partnership is exemplary for cooperation in the armed forces domain and represents an indispensable additional defense in this highly specialized field.

At the international level, Austria also participates in a number of other cyber-related initiatives, working most notably with the OSCE (above all during Austria's 2017 Chairmanship) and its confidence-building measures and high-level conferences (e.g. Cyber Security for Critical Infrastructure: Strengthening Confidence Building in the OSCE); the UN and its Global Forum on Cyber Expertise (GFCE); The Council of Europe; the World Summit on the Information Society (WSIS); the International Telecommunication Union (ITU) and its Global Cybersecurity Agenda initiative; and the Organization for Economic Co-operation and Development (OECD) and its international guidelines for cybersecurity, CIIP and SME digital risk management.

4.3 Cyberdefense awareness programs

There are no specific cyberdefense awareness programs mentioned in the policy documents examined. However, referring to the ICT security strategy, the NCSS calls for specific measures to further strengthen the Austrian ICT security and cybersecurity culture.[34] This has notably led to the development of a number of cybersecurity, ICT security and cybercrime awareness-raising initiatives, among them the **ICT security portal**, which went online in 2013. This web platform serves to raise awareness and acts as an information and communication hub for various target groups (i.e. users, customers and service providers). It was notably set up as an inter-ministerial initiative in cooperation with the Austrian business sector. Furthermore, a number of awareness campaigns have been developed alongside the platform, which draw on media articles, documentaries, brochures, conferences and e-learning programs (Digital Austria, 2012, p. 29). Among these is the **ICT Security Conference** organized by the BMLVS, which aims to sensitize managers above all to improve their awareness of potential threats. Other initiatives include various workshops organized by the CSP on a wide range of issues ranging from the NIS to the Austrian cybersecurity strategy 2.0, CERT activities, relevant exercises and beyond.[35] Moreover, awareness-raising programs directed at children have also been developed, among them the **Cyber.Kids** and **Click & Check** projects. Lastly, the Federal Ministry of Science, Research and Economy (BMWFW) coordinates a cybersecurity awareness program for SMEs (GovCert Austria & Cert.at, 2016, p. 39).

4.4 Cyberdefense education and training programs

All in all, very little information and details relating to cyberdefense and education programs can be found in public records. The Austrian Command Support School, together with its first and second battalions, has established so-called Cyber Training Centers, which are responsible for training cyber recruits, and the ÖSCS implementation report (BMLVS, BKA, BM.I, & BMEIA, 2016) refers to a number of additional initiatives. For instance, following the reform of the military service in 2014, an optional training module on cybersecurity was launched in the same year. In addition,

[34] An explicit reference is made to the 2012 National ICT security strategy and its awareness measures

[35] Please refer to https://www.digitales.oesterreich.gv.at/cyber-sicherheit-plattform#Veranstaltungen_der_CSP

general cyber awareness content for army recruits was developed, and recruits with special technical skills are now able to train as "cyber soldiers" (BMLVS, 2015, p. 7). Furthermore, a number of senior staff (at least 60 in 2015) of the Austrian Armed Forces were required to complete a special course on cybersecurity in cooperation with Hagenberg University of Applied Sciences.

In terms of cybersecurity education, it is worth noting that the Ministry for Education (BMBWF[36]) has developed its "efit21 for digital education" IT strategy. This document sets out a number of measures aimed at strengthening the digital and media skills (including data protection, data security and cybersecurity) of both students and educators. Relevant activities include rolling out the "Digikomp" initiative; communicating responsible behavior in the digital space through e-learning initiatives; developing topic-specific information and teaching materials as well as workshops for schools; and establishing additional qualifications for teachers in primary, secondary, further and continuing education at teacher training colleges (e.g. Virtual Teacher Training College).

4.5 Cyberdefense research programs

According to the 2012 White Paper, the research plan for 2012-2018 of the BMLVS central research center defines cybersecurity and cyberdefense as core topics. However, only very limited information has been published about the contents and results of such research. Both support battalions of the KdoFüU&CD operate their respective Cyber Defense Research Centers, which are responsible notably for developing methods and providing central ICT infrastructures, within the National Defense Academy in Vienna (2018 report, p. 33). The Austrian Armed Forces participate in the **Austrian National Security Research Program (KIRAS)**, which has set up over 30 projects relating to cybersecurity and cybercrime. Research topics include a secure cloud system, new malware detection methods and an e-government infrastructure, among others (BMLVS, 2015, p. 8). Furthermore, Austria takes part in the **Horizon 2020 program** and its various cybersecurity-related projects at the EU level.

[36] Bundesministerium für Bildung, Wissenschaft und Forschung

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 takes a defensive or offensive approach to cyberdefense.

As set out in the introduction to this collection, a state's position on these sliding scales is derived from the analysis conducted in the snapshots. For example, if a state focuses its policy development and implementation responsibilities significantly on just a few entities or even a single entity, it is reasonable to conclude that the relevant state takes a more centralized approach to cybersecurity and cyberdefense. Similarly, if responsibility for these sectors lies within the defense ministry, there will be a greater degree of military rather than civilian oversight, and if offensive cyberdefense capabilities are explicitly referred to in policy literature, a state can reasonably be assumed to take an offensive stance on cyberdefense, even if specific capabilities or tools are not mentioned.

5.1. Centralization vs decentralization of leadership

Diagram AT4: Spectrum of Centralization vs Decentralization of policy development and management

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

5.2. Civilian vs defense posture and oversight

Diagram AT5: Spectrum of Civilian-Defense cybersecurity posture and oversight

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

5.1 Offensive vs defensive capabilities

Diagram AT6: Spectrum of Offensive vs Defensive cyberdefense capabilities

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

6. Annex 2: Key definitions

The following key definitions are taken from the ÖCSC glossary:

Term	Definition
ICT security	ICT security is the protected state of information and communication technology and the information used therein which is appropriate to the type and level of sensitiveness as well as the type and intensity of a possible threat.
Information Security/network Security	Information security or network security are umbrella terms for ICT security, referring to the entire relevant information of an organization or an enterprise, including information that has not been processed electronically. Hence, it describes the entirety of characteristics of an organization ensuring the confidentiality, availability and integrity of information. Information may be available as spoken text, paper documents or other directly readable media or as electronically processed data in ICT systems.
Critical Information Infrastructure	Critical infrastructures are those infrastructures or parts thereof which are of crucial importance for ensuring important social functions. Their failure or destruction has severe effects on the health, security or the economic and social wellbeing of the population or the functioning of governmental institutions. Critical infrastructure is often abbreviated as CI (Critical Infrastructure) even in the German-language area. CIP has become the abbreviation commonly used at international and national level, referring to Critical Infrastructure Protection, while CIIP stands for Critical Information Infrastructure Protection.
Cyberattack	The term “cyberattack” refers to an attack through IT in cyberspace, which is directed against one or several IT system(s). Its aim is to undermine the objectives of ICT security protection (confidentiality, integrity and availability) partly or totally. Cyberattacks directed against the confidentiality of an IT system are referred to as “cyberespionage”, i.e. digital spying. Cyberattacks directed against the integrity and availability of an IT system are referred to as cyber sabotage.
Cyberspace	Cyberspace is the virtual space of all IT systems interconnected 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 may be supplemented and expanded through other data networks. In common parlance, cyberspace also refers to the global network of different independent IC infrastructures, telecommunication networks and computer systems. In the social sphere the use of this global network allows individuals to interact, exchange ideas, disseminate information, give social support, engage in business, control action, create art and media works, play games, participate in political discussions and a lot more. Cyberspace has become an umbrella term for all things related to the Internet and for different Internet cultures. Many countries regard networked ICT and independent networks operating through this medium as components of their “national critical infrastructures“.
Cybersecurity	Cybersecurity describes the protection of a key legal asset through constitutional means against actor-related, technical, organizational and natural dangers posing a risk to the security of cyberspace (including infrastructure and data security) as well as the security of the users in cyberspace. Cybersecurity helps to identify, assess and follow up on threats as well as to strengthen the ability to cope with interferences in or from cyberspace, to minimize the effects as well as to restore the capacity to act and functional capabilities of the respective stakeholders, infrastructures and services.
Cyberdefense	The term “cyberdefense” refers to all measures to defend cyberspace with military and appropriate means for achieving military-strategic goals. Cyberdefense is an integrated system, comprising the implementation of all measures relating to ICT and information security, the capabilities of milCERT and CNO (Computer Network Operations) as well as the support of the physical capabilities of the army.

Cyberwar	Cyberwar refers to acts of war in and around virtual space with means which are predominantly associated with information technology. In a broader sense, this implies the support of military campaigns in traditional operational spaces – i.e. ground, sea, air and outer space – through measures taken in the virtual space. In general, the term also refers to high-tech warfare in the information age based on the extensive computerization, electronization and networking of almost all military sectors and issues.
Data Protection	Every individual has a right to secrecy of his/her personal data, especially in terms of respect for his/her private and family life, provided that they represent interests worthy of protection. Data protection interests are excluded if the respective data are not subject to confidential treatment due to their general availability or lack of traceability to the individual affected.

6. Annex 3: Abbreviations

Abbreviation	English	German
AbwA	-	Abwehramt
A-SIT	Secure Information Technology Austria Center	Zentrum für sichere Informationstechnologie
ATC	Austrian Trust Circle	-
BAK	Federal Anti-Corruption Bureau	Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung
BKA	Federal Chancellery of Austria	Bundeskanzleramtes der Republik Österreich
BM.I	Federal Ministry of the Interior	Bundesministerium des Inneren
BMEIA	Federal Ministry for Europe, Integration and Foreign Affairs	Bundesministerium für Europa, Integration und Äußeres
BMLVS	Federal Ministry for National Defence and Sport	Bundesministerium für Landesverteidigung und Sport
BND	Federal Intelligence Service (Germany)	Bundesnachrichtendienst (Deutschland)
BVT	Federal Office for the Protection of the Constitution and Counterterrorism	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
C4	Cyber Crime Competence Center	-
CCDCOE	Cooperative Cyber Defence Centre of Excellence	-
CSS	Cybersecurity Steering Group	Cyber Sicherheit Steuerungsgruppe
CDC	Cyber Defense Center	Cyber Verteidigungszentrum
CSC	Cyber Security Center	Cyber Sicherheitszentrum
CSP	Austrian Cybersecurity Platform	-
CKM	Cyber Crisis Management	Cyber Krisenmanagement
D-A-CH	Germany-Austria-Switzerland	Deutschland-Österreich-Schweiz
EU	European Union	Europäische Union
FPÖ	Freedom Party of Austria	Freiheitliche Partei Österreichs
GovCERT	Government Computer Emergency Response Team	-
HNaA	Army Intelligence Office	Heeres-Nachrichtenamt
IAEA	International Atomic Energy Agency	-
IKT	Information and Communication Technology	Informations- und Kommunikationstechnologie
IKDOK	Inner Circle of the Operational Coordination Structure	Innerer Kreis der Operativen Koordinierungsstrukturen
KdoFüU&CD	Commando Communications and Cyber Defense	Kommando Führungsunterstützung und Cyber Defence

KIRAS	Austrian development plan for security research	Österreichisches Förderprogramm für die Sicherheitsforschung
KSÖ	-	Kuratorium Sicheres Österreich
MilCERT	Military Computer Emergency Readiness Team	-
MSK	Strategic military concept	Militärstrategisches Konzept
NATO	North Atlantic Treaty Organization	Nordatlantikpakt
NDB	Swiss intelligence agencies	Nachrichtendienst des Bundes
ÖBH	Austrian Armed Forces	Österreichisches Bundesheer
ÖSCS	Austrian strategy for cybersecurity	Österreichische Strategie für Cyber Sicherheit
ÖSS	Austria security strategy	Österreichische Sicherheitsstrategie
ÖVP	Austria people party	Österreichische Volkspartei
PfP	Partnership for Peace	-
SKKM	Governmental crisis and disaster management	Staatliches Krisen- und Katastrophenmanagement
TV	Partial strategy defense policy	Teilstrategie Verteidigungspolitik
ZIKTCySih	Center for ICT and Cyber Security	Zentrum für IKT- und Cybersicherheit

8. Bibliography

Austrian Trust Circle. (n.d.). The Austrian Trust Circle [Organization’s page]. Retrieved from https://www.austriantrustcircle.at/home/

BKA. (2013). Austrian Cyber Security Strategy. Bundeskanzleramt.

Blauensteiner, P. (n.d.). *Aktuelle Cyber-Lage Ein kleiner Überblick über aktuelle Cyber-Bedrohungen*. Retrieved from file:///C:/Users/scordey/Downloads/06-aktuelle_cyber-lage-blauensteiner.pdf

BMLVS. (2013). Weiss Buch 2012. BMLVS.

BMLVS. (2015). Militärstrategisches Konzept 2015. BMLVS.

BMLVS, BKA, BM.I, & BMEIA. (2016). Österreichische Strategie für Cyber Sicherheit (ÖSCS) Umsetzungsbericht 2015. Retrieved from https://www.onlinesicherheit.gv.at/service/initiativen_und_angebote/koordination_und_strategie/OeSCS_Bericht_2015.pdf?6p24mr

Cert.at. (2017, January 23). Die Österreichische Strategie für Cyber Sicherheit: Status quo und Ausblick. Retrieved from https://www.cert.at/reports/report_2016_chap05/content.html

Cyber Security Austria. (n.d.). Cybersecurity Austria [Organization’s page]. Retrieved from https://www.cybersecurityaustria.at/index.php/verein/ziele

Cyber Sicherheit Steuerungsgruppe. (2015). Berich Cyber Sicherheit 2015. BKA.

Cyber Sicherheit Steuerungsgruppe. (2017). Berich Cyber Sicherheit 2017. BKA.

Cyber Sicherheit Steuerungsgruppe. (2018). Berich Cyber Sicherheit 2018. BKA.

Cyberwiser. (n.d.). Austria. Retrieved from https://www.cyberwiser.eu/austria-au

Der Standard. (2009, January 12). “Conficker”-Wurm legte Landesregierung und Spitäler in Kärnten lahm [News media]. Retrieved from https://derstandard.at/1231151587065/Conficker-Wurm-legte-Landesregierung-und-Spitaeler-in-Kaernten-lahm

Digital Austria. (2012). National ICT Security Strategy Austria. BKA.

Digital Oesterreich. (n.d.). Cyber Sicherheit Plattform (CSP). Retrieved from https://www.digitales.oesterreich.gv.at/cyber-sicherheit-plattform

ENISA. (2017, November). Public Private Partnerships (PPP) Cooperative models. European Union Agency for Network and Information Security. Retrieved from file:///C:/Users/scordey/Downloads/WP2017%20O-3-1-3%203%20Public%20Private%20Partnerships%20-PPP-%20Cooperative%20models.pdf

European Cybersecurity Organisation. (2018, January). *European Cybersecurity in Public Private Partnership*. Vienna. Retrieved from https://www.energypact.org/wp-content/uploads/2018/03/Rebuffi_Day1_European-Cybersecurity-in-Public-Private-Partnership.pdf

European Defence Agency. (2017, May 12). Cyber Ranges: EDA’s First Ever Cyber Defence Pooling & Sharing Project Launched By 11 Member States [Organization’s page]. Retrieved from https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/05/12/cyber-ranges-eda-s-first-ever-cyber-defence-pooling-sharing-project-launched-by-11-member-states

European Defence Agency. (2018, June 28). Six Member States agree to pool & share cyber ranges capabilities [Organization’s page]. Retrieved from https://www.eda.europa.eu/info-hub/press-centre/latest-news/2018/06/28/six-member-states-agree-to-pool-share-cyber-ranges-capabilities

Federal Chancellery of the Republic of Austria. (2014). Cybersecurity report 2014. BKA.

GovCert Austria, & Cert.at. (2016, February). Bericht Internet-Sicherheit Österreich 2015 Gesamtausgabe. Cert.at.

Graz University. (n.d.). A-SIT - Secure Information Technology Center Austria [Organization’s page]. Retrieved from https://graz.pure.elsevier.com/en/projects/a-sit-secure-information-technology-center-austria

International Monetary Fund. (2018). World Economic Outlook Database, January 2018. International Monetary Fund. Retrieved from http://www.imf.org/external/pubs/ft/weo/2017/02/weodata/weorept.aspx?sy

ITU. (2017, July 19). Global Cybersecurity Index (GCI). ITU.

Jahn, G. (2013, September 13). Alleged NSA post in Austria becomes state affair [News media]. Retrieved from https://www.yahoo.com/news/alleged-nsa-post-austria-becomes-state-affair-124218174.html

Kirňák, M., Šulc, R., Illési, Z., & Gapiński, K. (2016). V4 GOES CYBER: CHALLENGES AND OPPORTUNITIES. Visegrad Fund. Retrieved from http://www.pssi.cz/download/docs/372_final-project-report.pdf

Kuratorium Sicheres Österreich. (n.d.). Cyber Security [Organization’s page]. Retrieved from https://kuratorium-sicheres-oesterreich.at/allgemein/cyber-security/

NATO. (2018). Austria. NATO Science for Peace and Security Programme. Retrieved from https://www.nato.int/science/country-fliers/Austria.pdf

Online Sicherheit.at. (2018, November 27). Cyber Crime Competence Center (C4). Retrieved from https://www.onlinesicherheit.gv.at/service/initiativen_und_angebote/beratung_und_sensibilisierung/71347.html

ORF news. (2018, March 14). Bundesheer receives less budget than announced [News media]. Retrieved from https://orf.at/v2/stories/2430127

Reuters. (2017a, February 7). Austrian parliament says Turkish hackers claim cyberattack [News media]. Retrieved from https://www.reuters.com/article/us-austria-hackers-parliament-idUSKBN15M0NX

Reuters. (2017b, July 7). Austrian parliament says Turkish hackers claim cyberattack [News media]. Retrieved from https://www.reuters.com/article/us-austria-hackers-parliament-idUSKBN15M0NX

Schmid, F. (2017, March 5). Die gefährliche Cyberrivalität zwischen Heer und Polizei [Newspaper]. Retrieved from https://derstandard.at/2000053486772/Die-gefaehrliche-Cyber-Rivalitaet-zwischen-Heer-und-Polizei

World Economic Forum. (2016). Networked Readiness Index. World Economic Forum. Retrieved from http://reports.weforum.org/global-information-technology-report-2016/networked-readiness-index/

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 towards 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

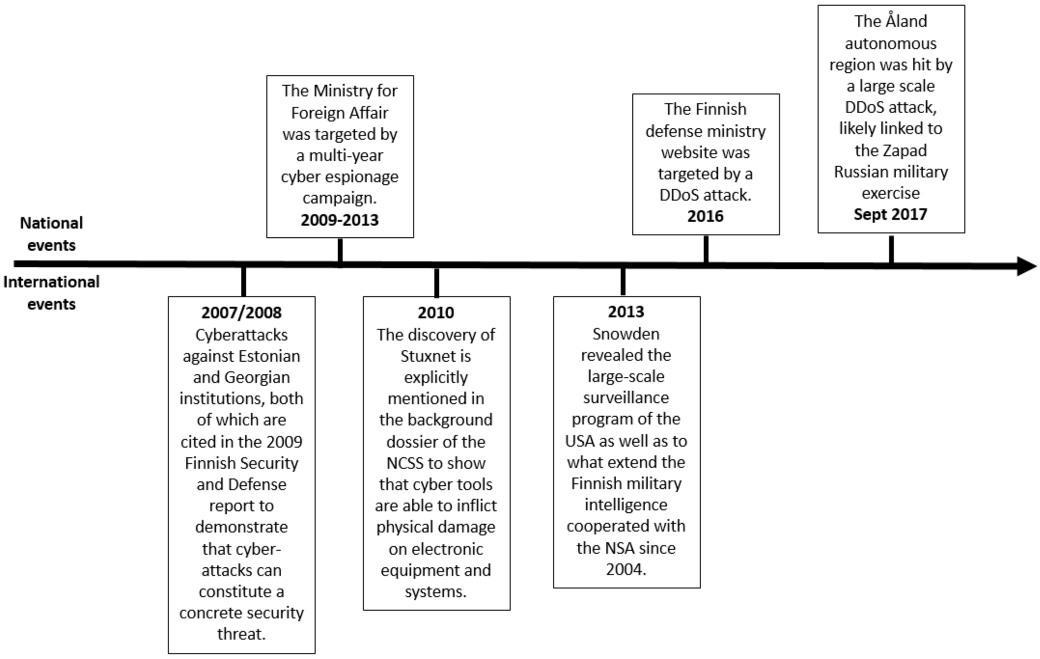
Finland's key international partners are its Nordic-Baltic neighbors (specifically NORDEFCO & NB8), the European Union (including the EDA, ENISA and cyber response teams) and – despite not being a member – NATO (through entities such as the CCDCOE, Hybrid CoE and cyberdefense exercises). Finland also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

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

1.1. Threat perceptions: trigger events

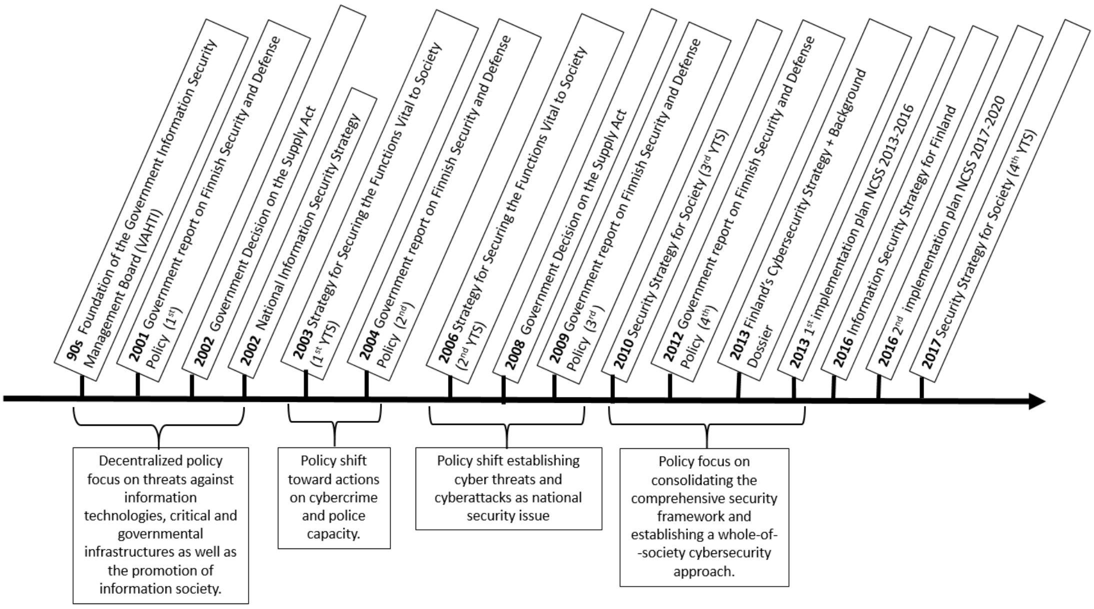
This sub-section describes the main domestic and international events that have had an impact on the shaping of cybersecurity and cyberdefense policies in Finland. It must be noted that no specific threats to Finland are explicitly mentioned in policy documents. However, the latest defense report recognizes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

Diagram FN1: Timeline of trigger events


National events
International events
The Ministry for Foreign Affair was targeted by a multi-year cyber espionage campaign. **2009-2013**
The Finnish defense ministry website was targeted by a DDoS attack. **2016**
The Åland autonomous region was hit by a large scale DDoS attack, likely linked to the Zapad Russian military exercise **Sept 2017**
2007/2008 Cyberattacks against Estonian and Georgian institutions, both of which are cited in the 2009 Finnish Security and Defense report to demonstrate that cyber-attacks can constitute a concrete security threat.
2010 The discovery of Stuxnet is explicitly mentioned in the background dossier of the NCSS to show that cyber tools are able to inflict physical damage on electronic equipment and systems.
2013 Snowden revealed the large-scale surveillance program of the USA as well as to what extend the Finnish military intelligence cooperated with the NSA since 2004.

1.2. Main policy documents: key shifts in strategy

Diagram FN2: Timeline of policy developments and trends


90s Foundation of the Government Information Security Management Board (VAHTI)
2001 Government report on Finnish Security and Defense Policy (1st)
2002 Government Decision on the Supply Act
2002 National Information Security Strategy
2003 Strategy for Securing the Functions Vital to Society (1st YTS)
2004 Government report on Finnish Security and Defense Policy (2nd)
2006 Strategy for Securing the Functions Vital to Society (2nd YTS)
2008 Government Decision on the Supply Act
2009 Government report on Finnish Security and Defense Policy (3rd)
2010 Security Strategy for Society (3rd YTS)
2012 Government report on Finnish Security and Defense Policy (4th)
2013 Finland's Cybersecurity Strategy + Background Dossier
2013 1st implementation plan NCSS 2013-2016
2016 Information Security Strategy for Finland
2016 2nd implementation plan NCSS 2017-2020
2017 Security Strategy for Society (4th YTS)
Decentralized policy focus on threats against information technologies, critical and governmental infrastructures as well as the promotion of information society.
Policy shift toward actions on cybercrime and police capacity.
Policy shift establishing cyber threats and cyberattacks as national security issue
Policy focus on consolidating the comprehensive security framework and establishing a whole-of--society cybersecurity approach.

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.[37] 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[38]). The coordination of cybersecurity preparedness is led by the Security Committee (TK[39]), 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 towards 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[40], 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[41] 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, cyberthreats, cyberespionage 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.).[42] 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

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

[38] Valtioneuvoston ulko- ja turvallisuuspoliittinen ministerivaliokunta.

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

[40] 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.

[41] "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).

[42] 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.

information society and economy. As such, the protection of information, its systems and other digital assets as well as 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 cyberespionage cases. Indeed, before the 2010 Security Strategy for Society (YTS 2010[43]) and the 2013 NCSS, information security, cyberdefense, critical information infrastructure protection and the promotion of digital industry had instead operated in their respective silos.

[43] Yhteiskunnan turvallisuusstrategia.

2. Current cybersecurity policy

2.1. Overview of key policy documents

2.1.1. 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 – cyberthreats" (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.

2.1.2. 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[44] 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*.[45]

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 (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.

2.2. 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:

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

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

1. Finland can **secure its vital functions against cyberthreats** in all situations.
2. Citizens, the authorities and businesses can effectively **utilize a safe cyber domain** and the competence arising from cybersecurity measures, both nationally and internationally.
3. (By 2016)[46] Finland will be a **global forerunner in cyberthreat 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 cyberthreats 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 cybersecurity measures through national legislation
9. Assign cybersecurity-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.

2.3. National cyberdefense 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[47], 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 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.

2.4. 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

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

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

tasks. Meanwhile, its coordination and monitoring are under the auspice of the TK, a body chaired by a military officer[48] (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 cyber warfare 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.[49] 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[50] (ITU, 2017). It is also the fourth most digitally 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 cyberpowers are pursuing (i.e. USA, Russia or China[51]). 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 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.

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

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

[50] 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.

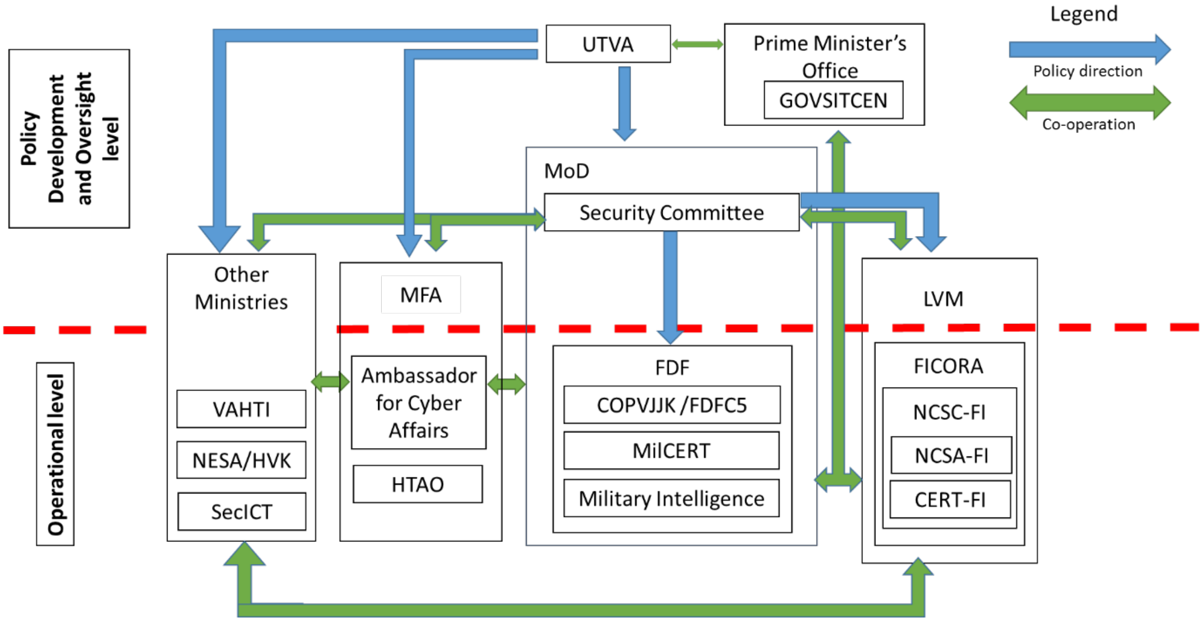
[51] For instance, setting up a cyber command or a centralized expert cyber center.

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.[52] 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 in addition to promoting national and international cooperation in the field (Manuel Suter and Elgin Brunner, 2008). Under the terms of the 2013 NCSS, FICORA also hosts the new National Cyber Security Centre (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:

[52] 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

1. Compile and disseminate the cybersecurity situation picture in close cooperation with its support network
2. Compile and maintain a cyberthreat 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 fora, 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 cyberthreat-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[53]),** under the ministry of Finance, is responsible for steering, developing, coordinating and harmonizing the central government information security[54] 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 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 cyberthreats against the continuity of

[53] The julkisen hallinnon digitaalisen turvallisuuden johtoryhmä.

[54] See definition section for more details.

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.[55]

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.[56] Its operational arm is the **Finnish Defense Forces C5 Agency** (PVJJK[57]/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 cyberdefense and the FDF's cyber situational awareness. In addition, it develops cyberdefense 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).

3.4. Context: key public organizational framework

The Finnish cyberarchitecture 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.

[55] 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.

[56] Johtamisjärjestelmäosasto

[57] Puolustusvoimien johtamisjärjestelmäkeskus

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[58] – 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).[59]

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 cybersecurity 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.

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

[59] 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 cybersecurity 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 towards 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 cyberdefense capabilities based on enhanced information sharing, identifying best practice, computer emergency responses and regular cybersecurity-based defense exercises (Gerard O'Dwyer, 2017). The NORDEFCO members therefore conduct technical cooperation, joint cybersecurity 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.[60] 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

[60] 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 cyberdefense.

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 cybersecurity.

4.3. Cyberdefense 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 cyberdefense 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[61]) 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 cyberdefense and electronic warfare systems (The Finnish Defence Forces, n.d.).

On the civilian side, Business Finland (TEKES[62]) and the Academy of Finland have, according to the NCSS, developed a **strategic research agenda** 2014-2017 for cyber (i.e. cyber trust[63]). 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.

[61] Aka. TIVIT or DIGILE

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

[63] 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).
Cybersecurity	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 cyberthreats and, should they still materialize, prevent, mitigate or help tolerate their consequences. Note 3 Cybersecurity 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 cyberthreats and their effects, which can cause significant harm or danger to Finland or its population.
Cyberdefense[64]	The national defense-related sector of cybersecurity, which incorporates the capabilities of intelligence, surveillance, cyberattack and cyberdefense.
Information (data) security	Information security means the administrative and technical measures taken to ensure the availability, integrity and confidentiality of data.
Cyberthreat	Cyberthreat means the possibility of action or an incident in the cyber domain which, when materialized, jeopardizes some operation dependent on the cyber world. Note Cyberthreats are information threats which, when materialized, jeopardize the correct or intended functioning of the information system.

[64] 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.

France

Marie Baezner
Center 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

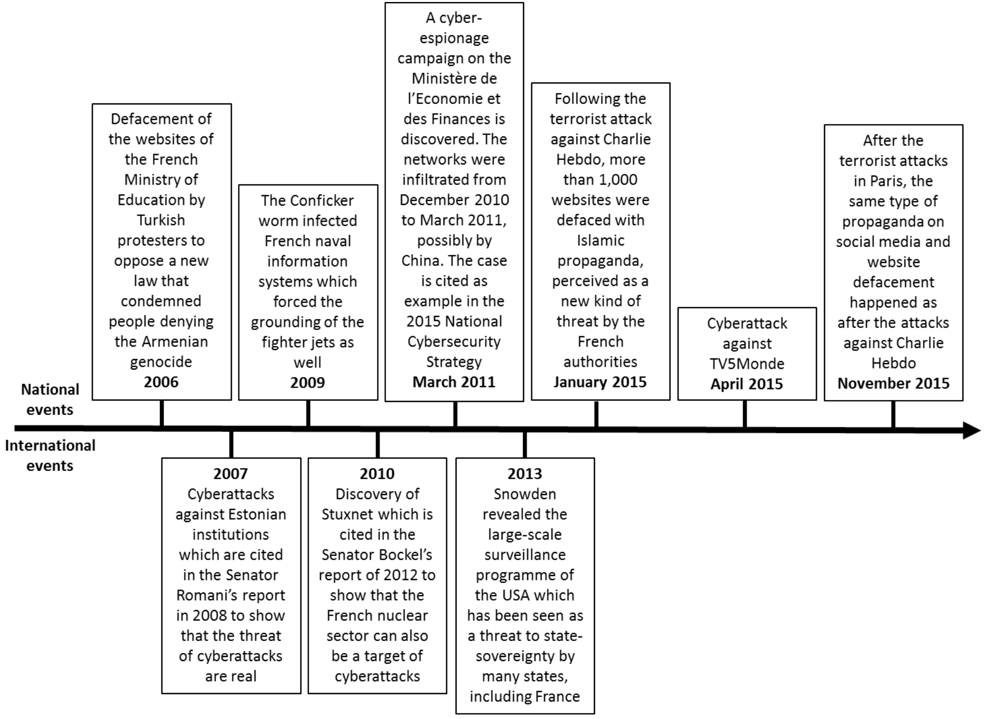
France cooperates on cybersecurity issues with its allies within NATO and the EU, but also wants to cooperate more closely with the UK and Germany on issues of cybersecurity. The strategies do not describe any public-private partnership, but the ANSSI is the main actor to set cybersecurity standards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



National events

Defacement of the websites of the French Ministry of Education by Turkish protesters to oppose a new law that condemned people denying the Armenian genocide **2006**

The Conficker worm infected French naval information systems which forced the grounding of the fighter jets as well **2009**

A cyber-espionage campaign on the Ministère de l'Economie et des Finances is discovered. The networks were infiltrated from December 2010 to March 2011, possibly by China. The case is cited as example in the 2015 National Cybersecurity Strategy **March 2011**

Following the terrorist attack against Charlie Hebdo, more than 1,000 websites were defaced with Islamic propaganda, perceived as a new kind of threat by the French authorities **January 2015**

Cyberattack against TV5Monde **April 2015**

After the terrorist attacks in Paris, the same type of propaganda on social media and website defacement happened as after the attacks against Charlie Hebdo **November 2015**

International events

2007 Cyberattacks against Estonian institutions which are cited in the Senator Romani's report in 2008 to show that the threat of cyberattacks are real

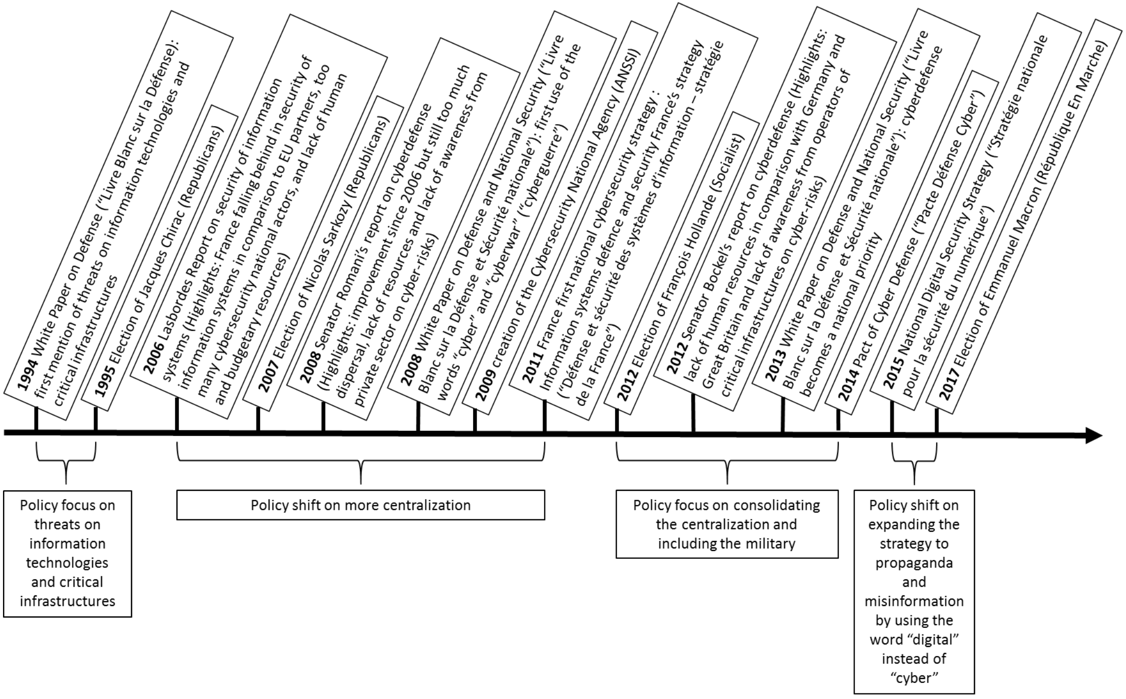
2010 Discovery of Stuxnet which is cited in the Senator Bockel's report of 2012 to show that the French nuclear sector can also be a target of cyberattacks

2013 Snowden revealed the large-scale surveillance programme of the USA which has been seen as a threat to state-sovereignty by many states, including France

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



1994 White Paper on Defense ("Livre Blanc sur la Défense): first mention of threats on information technologies and critical infrastructures

1995 Election of Jacques Chirac (Republicans)

2006 Lasbordes Report on security of information systems (Highlights: France falling behind in security of information systems in comparison to EU partners, too many cybersecurity national actors, and lack of human and budgetary resources)

2007 Election of Nicolas Sarkozy (Republicans)

2008 Senator Romani's report on cyberdefense (Highlights: improvement since 2006 but still too much dispersal, lack of resources and lack of awareness from private sector on cyber-risks)

2008 White Paper on Defense and National Security ("Livre Blanc sur la Défense et Sécurité nationale"): first use of the words "cyber" and "cyberwar" ("cyberguerre")

2009 creation of the Cybersecurity National Agency (ANSSI)

2011 France first national cybersecurity strategy : Information systems defence and security France's strategy ("Défense et sécurité des systèmes d'information – stratégie de la France")

2012 Election of François Hollande (Socialist)

2012 Senator Bockel's report on cyberdefense (Highlights: lack of human resources in comparison with Germany and Great Britain and lack of awareness from operators of critical infrastructures on cyber-risks)

2013 White Paper on Defense and National Security ("Livre Blanc sur la Défense et Sécurité nationale"): cyberdefense becomes a national priority

2014 Pact of Cyber Defense ("Pacte Défense Cyber")

2015 National Digital Security Strategy ("Stratégie nationale pour la sécurité du numérique")

2017 Election of Emmanuel Macron (République En Marche)

Policy focus on threats on information technologies and critical infrastructures

Policy shift on more centralization

Policy focus on consolidating the centralization and including the military

Policy shift on expanding the strategy to propaganda and misinformation by using the word "digital" instead of "cyber"

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[65]

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[66]

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).[67] 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 Cyberdefense 2014 (see Section 2.1.3).

2.1.3. Pact of Cyberdefense 2014[68]

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

[65] 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.

[66] Stratégie Nationale pour la Sécurité du Numérique, 2015

[67] Défense et sécurité des systèmes d'information – stratégie France, 2011

[68] 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.[69]

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.

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

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.
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 cyber-operations 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. While 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 Cyberdefense 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.

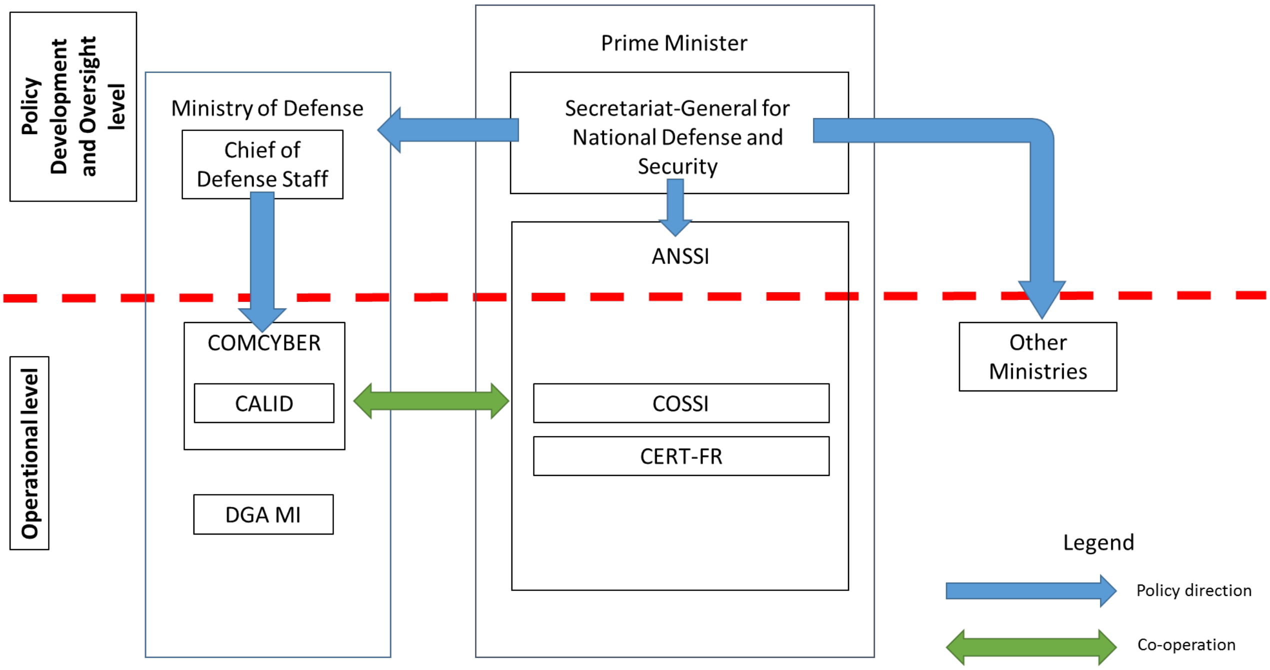
The wording adopted by the National Digital Security Strategy of 2015 and the Strategic Review of 2017 – the use of "digital" rather than "cyber" – demonstrates the willingness to broaden the understanding of cybersecurity issues and marks a shift in French strategic discourse, even in the field of defense policy. It shows a desire to shift from a restrictive *cyber warfare* 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 cyber-operations. COMCYBER is tasked with conducting cyberintelligence, 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[70] (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 cyberthreats, 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.

[70] 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 offense 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.

Germany

Patrice Robin
Center 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 cooperation 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 cyberthreats. 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 cyberterrorism 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 cyberattack.

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 cybersecurity research center.

4. Level of partnership and resources

Germany cooperates 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.

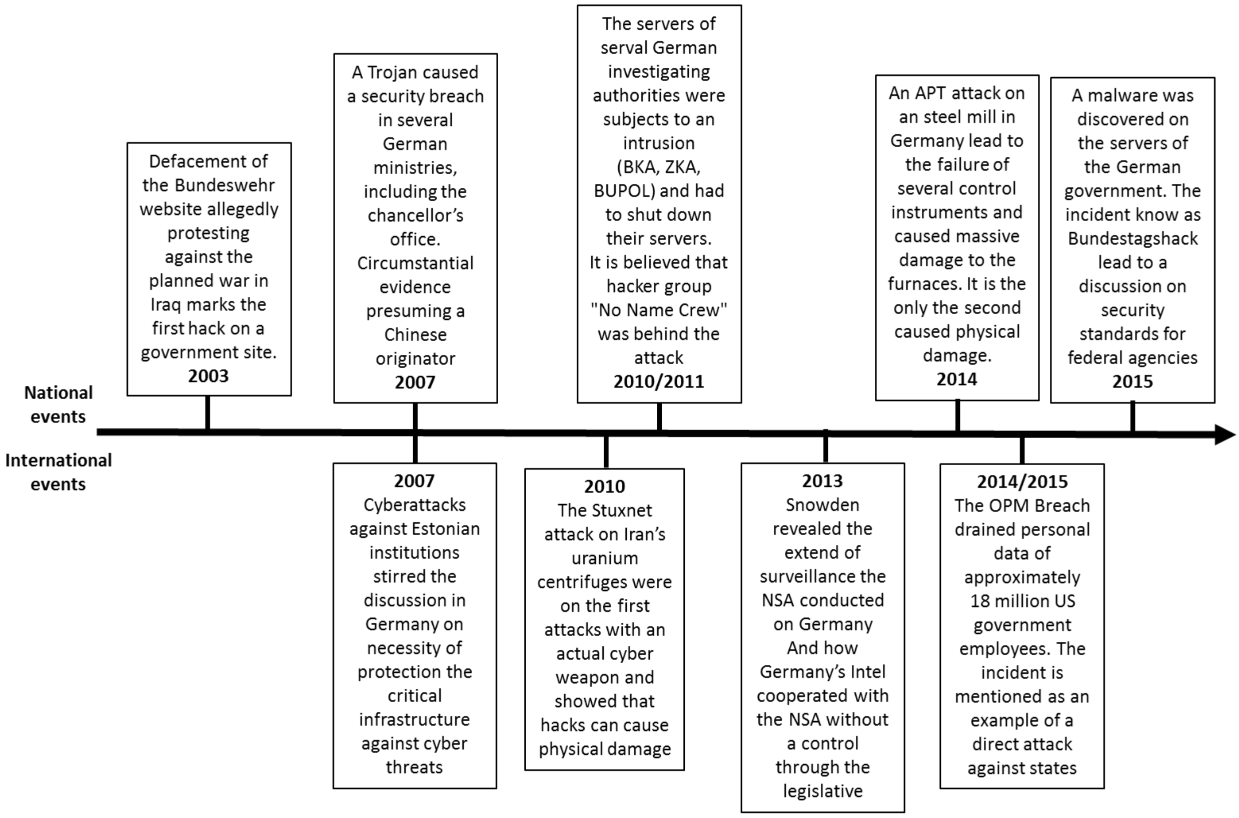
In cyberdefense Germany is an active member of the NATO Cooperative Cyberdefense Center of Excellence in Tallinn.

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



Defacement of the Bundeswehr website allegedly protesting against the planned war in Iraq marks the first hack on a government site. **2003**

A Trojan caused a security breach in several German ministries, including the chancellor's office. Circumstantial evidence presuming a Chinese originator **2007**

The servers of serval German investigating authorities were subjects to an intrusion (BKA, ZKA, BUPOL) and had to shut down their servers. It is believed that hacker group "No Name Crew" was behind the attack **2010/2011**

An APT attack on an steel mill in Germany lead to the failure of several control instruments and caused massive damage to the furnaces. It is the only the second caused physical damage. **2014**

A malware was discovered on the servers of the German government. The incident know as Bundestagshack lead to a discussion on security standards for federal agencies **2015**

2007 Cyberattacks against Estonian institutions stirred the discussion in Germany on necessity of protection the critical infrastructure against cyber threats

2010 The Stuxnet attack on Iran's uranium centrifuges were on the first attacks with an actual cyber weapon and showed that hacks can cause physical damage

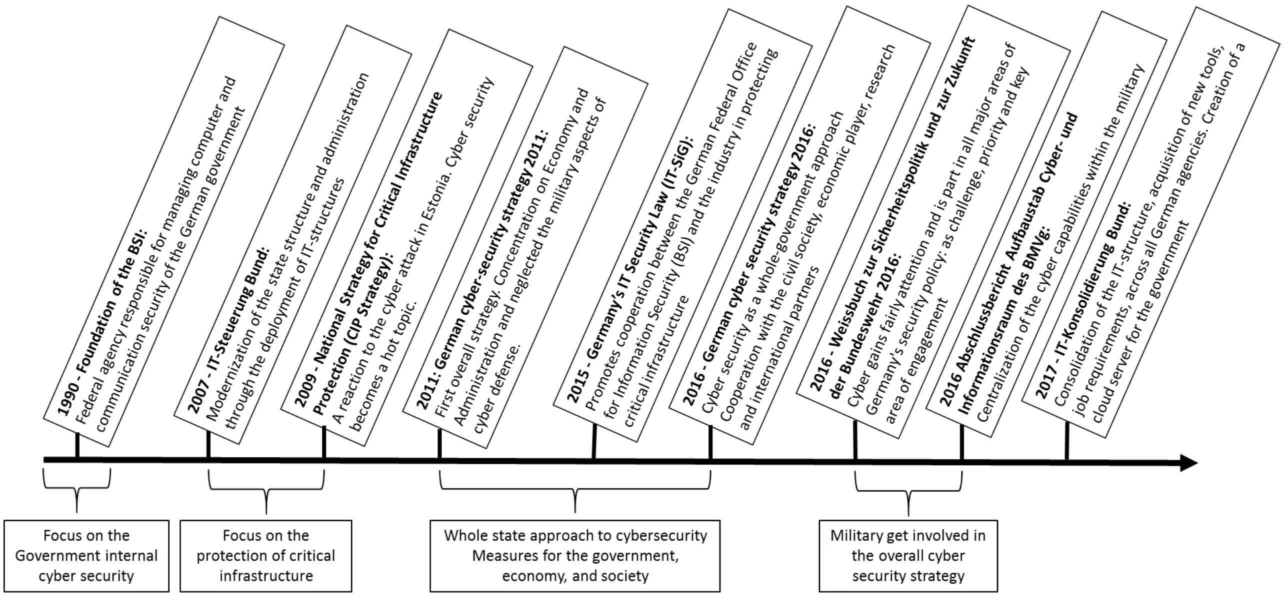
2013 Snowden revealed the extend of surveillance the NSA conducted on Germany And how Germany's Intel cooperated with the NSA without a control through the legislative

2014/2015 The OPM Breach drained personal data of approximately 18 million US government employees. The incident is mentioned as an example of a direct attack against states

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


1990 - Foundation of the BSI:
Federal agency responsible for managing computer and communication security of the German government
2007 - IT-Steuerung Bund:
Modernization of the state structure and administration through the deployment of IT-structures
2009 - National Strategy for Critical Infrastructure Protection (CIP Strategy):
A reaction to the cyber attack in Estonia. Cyber security becomes a hot topic.
2011: German cyber-security strategy 2011:
First overall strategy. Concentration on Economy and Administration and neglected the military aspects of cyber defense.
2015 - Germany's IT Security Law (IT-SiG):
Promotes cooperation between the German Federal Office for Information Security (BSI) and the industry in protecting critical infrastructure
2016 - German cyber security strategy 2016:
Cyber security as a whole-government approach Cooperation with the civil society, economic player, research and international partners
2016 - Weissbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr 2016:
Cyber gains fairly attention and is part in all major areas of Germany's security policy: as challenge, priority and key area of engagement
2016 Abschlussbericht Aufbaustab Cyber- und Informationsraum des BMVg:
Centralization of the cyber capabilities within the military
2017 - IT-Konsolidierung Bund:
Consolidation of the IT-structure, acquisition of new tools, job requirements, across all German agencies. Creation of a cloud server for the government
Focus on the Government internal cyber security
Focus on the protection of critical infrastructure
Whole state approach to cybersecurity Measures for the government, economy, and society
Military get involved in the overall cyber security strategy

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[71] (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

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

in Bosnia and Herzegovina in 1995, the deployment of troops in Afghanistan in 2003, patrolling the Aegean Sea in 2016, 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 cyberattacks. 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 ten 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)[72] 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.

[72] 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[73] (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.

[73] Zentralen Stelle für Informationstechnik im Sicherheitsbereich

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 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.

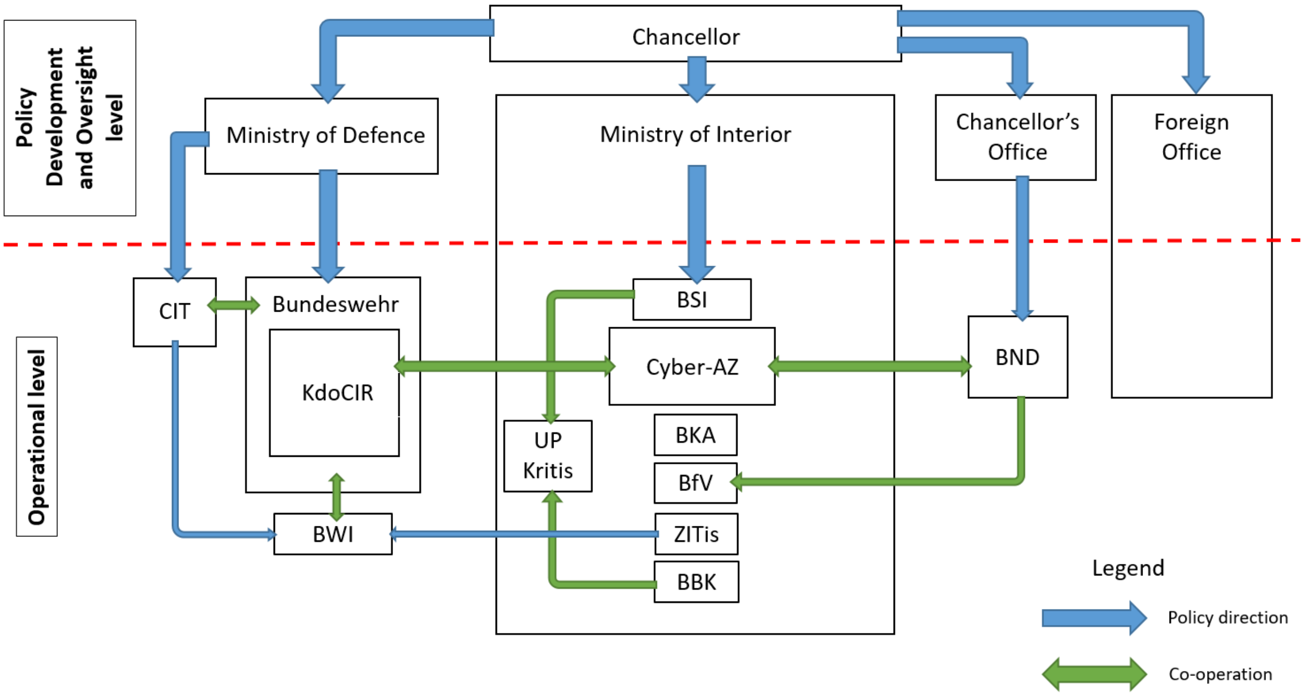
There is one element of German policy which merits particular attention. Because of the clear defensive posture set out in the policy documents examined, as well as an historic reticence to be seen to be projecting any form of hard power, it is surprising that Germany states in the AACI that it will 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 intergovernmental 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 cyberattack (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 cyberattacks 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 cyberattacks
- The intergovernmental 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 cyberattacks 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 cybersecurity (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).

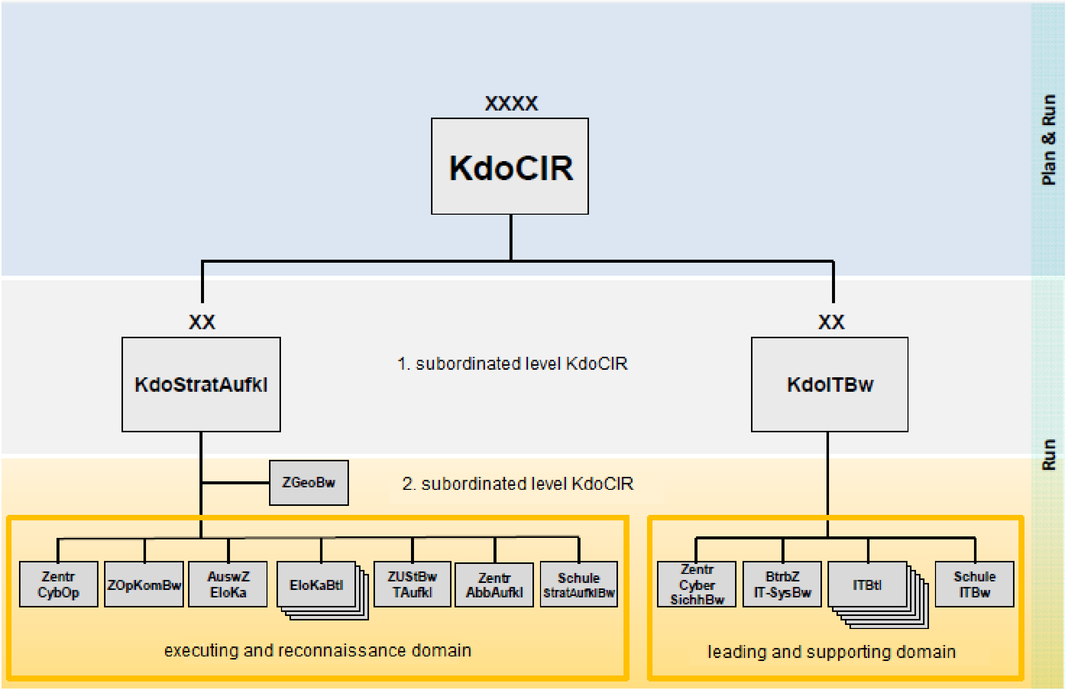
To achieve its goals, the KdoCIR includes a number of distinct entities. There are:

- 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 geoinformation 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 cyberattacks.
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 nationwide 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) cyberattacks.

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 non-military 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 cyberdefense 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:

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 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 cybersecurity	Civilian cybersecurity 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 cyberattack 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 "cyberdefense": ▪ "Cyberdefense" 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	Cyberattacks directed against the confidentiality of an IT system, which are launched or managed by foreign intelligence services.
Cybersabotage	Cyberattacks against the integrity and availability of IT systems (BMI, 2016, p. 9).
Cybersecurity	(Global) cybersecurity is the desired objective of the IT security situation, in which the risks of global cyberspace have been reduced to an acceptable minimum. Hence, cybersecurity 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. Cybersecurity (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 cybersecurity	Military cybersecurity 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).

Italy

Matteo Bonfanti
Center for Security Studies
ETH Zürich

Highlights/Summary:

1. Key national trends

Over the last 10 years, cybersecurity and cyberdefense have gained increasing importance in the Italian internal and external political agenda. They have been the objects of policies coupled with investment programs, which allowed Italy to take concrete actions to strengthen its national cyber preparedness and response mechanisms. With regard to the defense and military sector, Italy has established and is further developing cyberdefense capabilities to protect its interests and assets from cyberthreats, and conduct operations under the overall coordination of NATO, the EU and forces of allied countries.

2. Key policy principles

2.1 Cybersecurity

The Italian cybersecurity strategy sets out the goals, principles and guidelines that inform the actions to be taken by Italy for promoting its national cyber and ICT security. It also defines the institutional, organizational and procedural framework that should allow the Country to safeguard its economic, social, scientific and industrial development as well as political and military stability from cyberthreats. The strategy endorses a defensive, resilience- and response-based- rather than offensive cybersecurity posture. It outlines a reactive/response system aimed at protecting actively and in-depth the Italian cyber-related interests and assets from cyberthreats and attacks.

2.2 Cyberdefense

The Italian cybersecurity strategy also addresses issues pertaining to cyberdefense i.e. the protection, resilience and efficiency of military command and control networks as well as the acquisition and development of cyber capabilities to be deployed for military purposes.

3. Key national framework

3.1 Cybersecurity

In Italy, the implementation of the cybersecurity strategy relies on the active contribution of several governmental agencies, private organizations and the academia, who overall compose the Italian cybersecurity architecture. Due to the multitude of actors involved, coordination and cooperation among them remains crucial. These are assured by those civilian organisms which play core roles in the field of cybersecurity.

3.2 Cyberdefense

The MoD and its military structures are responsible for securing military networks and systems as well supporting military operations in cyberspace for defense purposes. They also concur to defend national critical infrastructures and assets from cyberattacks that may exceed the response capacity of civilian agencies.

4. Level of partnership and resources

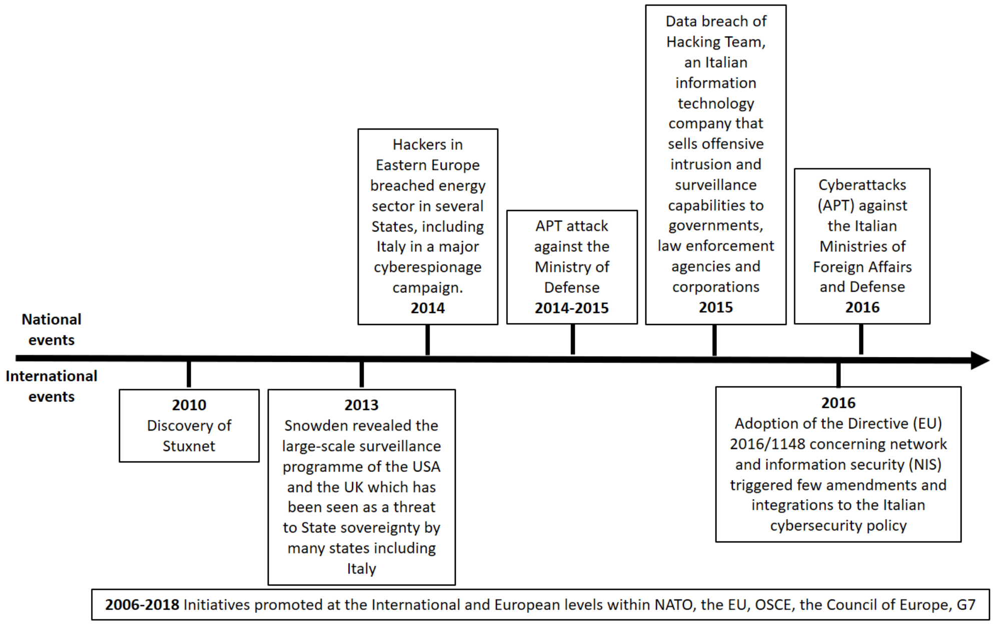
At the international and regional level, Italy favors cooperation on cybersecurity with the UN, G7, NATO, OSCE and the EU. At the domestic level, it also strongly supports public-private partnership initiatives that are aimed at promoting the national interests in and through the cyberspace, and safeguarding the Country’s critical assets.

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

1.1 Threat perception: trigger events

This section describes the main domestic and international events that had an impact on the shaping of cybersecurity and cyberdefense policies in Italy. In general, there are no specific threats mentioned in the Italian policy documents that triggered policy initiatives or developments. These documents mainly refer to international initiatives promoted by the NATO, UE, OCSE, the Council of Europe, or within other intergovernmental fora, which prompted Italy to take actions in the field of cybersecurity and cyberdefense. However, there are few events that are often mentioned among community of practitioners and, in general, the media, which boosted the process for adoption of policies and measures aimed at improving cybersecurity in Italy.

Diagram ITA1: Timeline of trigger events



National events

Hackers in Eastern Europe breached energy sector in several States, including Italy in a major cyberespionage campaign. **2014**

APT attack against the Ministry of Defense **2014-2015**

Data breach of Hacking Team, an Italian information technology company that sells offensive intrusion and surveillance capabilities to governments, law enforcement agencies and corporations **2015**

Cyberattacks (APT) against the Italian Ministries of Foreign Affairs and Defense **2016**

International events

2010 Discovery of Stuxnet

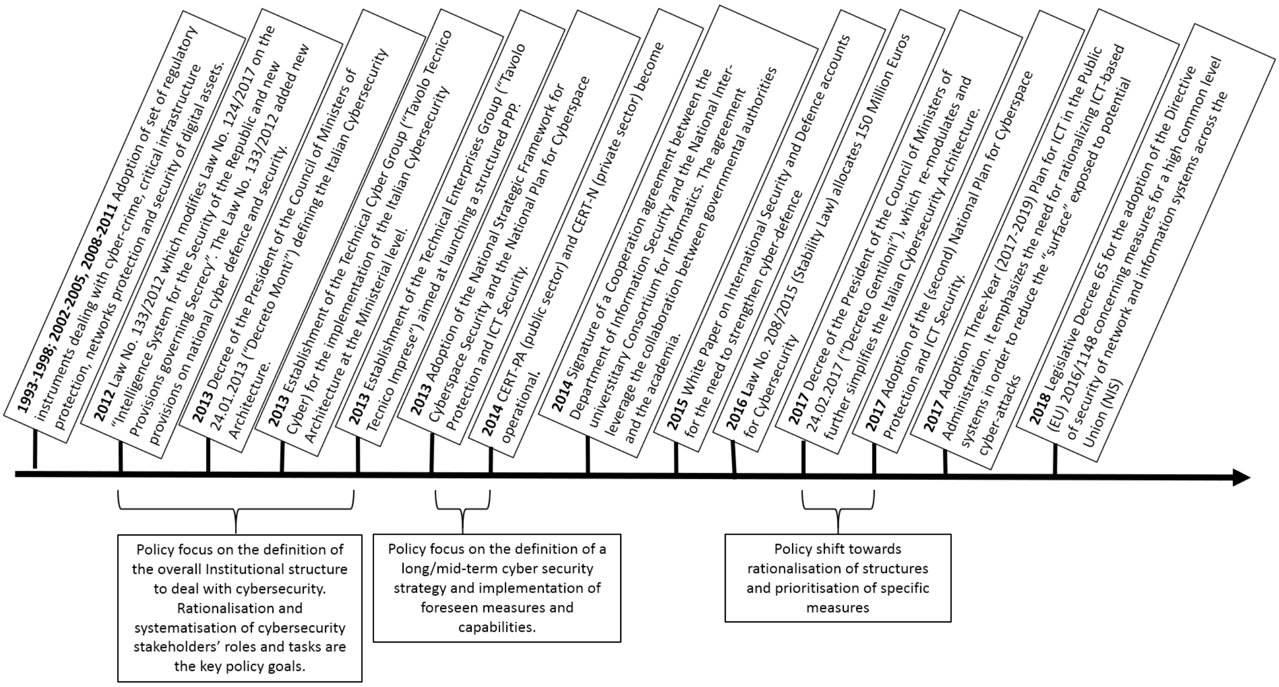
2013 Snowden revealed the large-scale surveillance programme of the USA and the UK which has been seen as a threat to State sovereignty by many states including Italy

2016 Adoption of the Directive (EU) 2016/1148 concerning network and information security (NIS) triggered few amendments and integrations to the Italian cybersecurity policy

2006-2018 Initiatives promoted at the International and European levels within NATO, the EU, OSCE, the Council of Europe, G7

1.1 Main Policy Documents: Key Shifts in Strategy

Diagram ITA2: Timeline of policy developments and trends



1993-1998; 2002-2005, 2008-2011 Adoption of set of regulatory instruments dealing with cyber-crime, critical infrastructure protection, networks protection and security of digital assets.

2012 Law No. 133/2012 which modifies Law No. 124/2017 on the "Intelligence System for the Security of the Republic and new Provisions governing Secrecy". The Law No. 133/2012 added new provisions on national cyber defence and security.

2013 Decree of the President of the Council of Ministers of 24.01.2013 ("Decreto Monti") defining the Italian Cybersecurity Architecture.

2013 Establishment of the Technical Cyber Group ("Tavolo Tecnico Cyber) for the implementation of the Italian Cybersecurity Architecture at the Ministerial level.

2013 Establishment of the Technical Enterprises Group ("Tavolo Tecnico Imprese") aimed at launching a structured PPP.

2013 Adoption of the National Strategic Framework for Cyberspace Security and the National Plan for Cyberspace Protection and ICT Security.

2014 CERT-PA (public sector) and CERT-N (private sector) become operational.

2014 Signature of a Cooperation agreement between the Department of Information Security and the National Inter-universitary Consortium for Informatics. The agreement leverage the collaboration between governmental authorities and the academia.

2015 White Paper on International Security and Defence accounts for the need to strengthen cyber-defence

2016 Law No. 208/2015 (Stability Law) allocates 150 Million Euros for Cybersecurity

2017 Decree of the President of the Council of Ministers of 24.02.2017 ("Decreto Gentiloni"), which re-modulates and further simplifies the Italian Cybersecurity Architecture.

2017 Adoption of the (second) National Plan for Cyberspace Protection and ICT Security.

2017 Adoption Three-Year (2017-2019) Plan for ICT in the Public Administration. It emphasizes the need for rationalizing ICT-based systems in order to reduce the "surface" exposed to potential cyber-attacks

2018 Legislative Decree 65 for the adoption of the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS)

Policy focus on the definition of the overall Institutional structure to deal with cybersecurity. Rationalisation and systematisation of cybersecurity stakeholders' roles and tasks are the key policy goals.

Policy focus on the definition of a long/mid-term cyber security strategy and implementation of foreseen measures and capabilities.

Policy shift towards rationalisation of structures and prioritisation of specific measures

1.2 Organizational structures: key parameters

The Italian cybersecurity policy has the goal to support Italy in pursuing its national interests in and through the cyberspace. The implementation of the policy relies on the active contribution of several governmental agencies, private organizations and the academia, who overall compose the Italian "cybersecurity architecture". From an organizational perspective, the strategic leadership of, and ultimate responsibility for, all aspects of cybersecurity lies with the Prime Minister who exercises it through structures and functions established within the Presidency of the Council of Ministers. Reference is primarily made to the Department of Information Security (DIS) who is in charge – together with other agencies – of the intelligence function for the Italian decision and policy makers. Other Ministries – in particular, the Home Affairs, Economic Development, Defence, Foreign Affairs, Justice, and Economy – have a significant stake in the definition of the cybersecurity policy and actively support the Prime Minister's strategic direction. This makes the Italian policy and institutional framework governing cybersecurity a hybrid version between a centralized and decentralized/distributed model.

To note that cyberdefense is part of the overall cybersecurity policy. Operational capabilities are distributed between the civil and military, with a heavy weighting towards civilian guidance and oversight. Military cyber capabilities are deployed to secure military networks and systems as well as to support military operations in cyberspace; they complement the civilian ones when necessary.

1.3 Context/Analysis: key national trends

Italy is a mid-sized power who takes part in to several universal and regional intergovernmental organizations and cooperation frameworks, ranging from the United Nations, the Organisation of Economic Cooperation and Development, the European Union, the Council of Europe to the G7 and G20. Geographically positioned at the heart of the Euro-African continents, Italy has traditionally articulated its foreign policy around three main subjects: Europe, the Mediterranean, and the transatlantic partnership – the latter incentivized through participating to the NATO cooperation framework. As a member of the European Union, Italy contributes to shaping the EU policies and initiatives in many areas. With regard to the Mediterranean region, Italy is primarily confronted with issues concerning migration, energy security, terrorism and organized crime, as well as the need to promote social and economic prosperity and security. The Italian-US cultural, political and economic relations remain critically important for Italy. They occur at both bilateral level and within the NATO partnership.

With regard to the cyberspace and its use by State and non-state actors, Italy regularly participates in international negotiations and dialogues aimed at fostering cooperation in this field. For example, it takes part to fora discussing the promotion of responsible State behavior in cyberspace, the development of a fundamental rights compliant digital economy, and the shaping of a free and inclusive Internet. Italy's approach towards the above-mentioned topics is premised upon the awareness of the strategic importance of cyberspace for the economic, social and cultural development of the Country. It is furthermore based on the acknowledgment of the national security and public order implications originating from the use of cyberspace.

In this respect, over the last 10 years, cybersecurity and cyberdefense have gained increasing importance in the Italian internal and external political agenda. Accordingly, they have been the objects of policies coupled with investment programs, which allowed Italy to take concrete actions to strengthen its national cyber preparedness and response mechanisms. In particular, Italy established a national incident response system, a cyber crisis management mechanism; it set up ad hoc bodies to fight cybercrime, created platforms for sustaining partnerships between governmental agencies, private organizations and the academia, funded research and development programs in cybersecurity, sustained campaigns aimed at raising public awareness about cyberthreats and cyber hygiene. With regard to the defense and military sector, Italy has established cyber defense capabilities.

As per the latter, their acquisition and further development are seen as prerequisites to face the challenged posed by the hybrid nature of modern conflicts. They have been and are considered the instruments to conduct cyber defense activities under the overall coordination of NATO, the EU and forces of allied and friendly countries.

2. Current cybersecurity policy

2.1 Overview of key policy documents

The Italian cybersecurity policy is defined by a set of legal and programmatic instruments that have been adopted and implemented at the Governmental level since early 2013. These instruments establish the strategic and operational goals pursued by Italy with regard to the secure use of the cyberspace; they also outline the activities to be promoted by selected national actors in order to achieve these goals. Overall, the above instruments design the Italian cybersecurity strategy and institutional architecture, which are both aimed at allowing Italy to pursue its national interests in and through the cyberspace.

The Italian cybersecurity policy is mainly civilian-lead and civilian-oriented. That means cybersecurity is mostly governed by civilian agencies and aims at safeguarding the Country's economic growth, social stability and national security. Nevertheless, the Italian cybersecurity policy also addresses issues pertaining to cyberdefense i.e. the protection, resilience and efficiency of military command and control networks as well as the acquisition and development of cyber capabilities to be deployed for military purposes.

2.1.1 The 2014 National Strategic Framework for Cyberspace Security and the National Plan for Cyberspace Protection and ICT Security

The National Strategic Framework for Cyberspace Security (NSF) and the associated National Plan for Cyberspace Protection and ICT Security (NP cyber) provide the strategic and operational guidelines (in Italian: "indirizzi") to enhance cybersecurity in Italy.[74] Published in 2014, both instruments are the result of an inclusive consultation process which involved several national administrations. The NSF and NP cyber are premised upon the adoption of the Decree of the President of the Council of Ministers of 24 January 2013, which represents the foundation stone of the Italian cybersecurity institutional architecture.[75] The Decree, also known as "Decreto Monti" (from the name of the Italian Prime Minister at that time), promoted the initial rationalization and systematization of the remits and functions concerning cybersecurity and critical infrastructures protection in Italy, which, until then, were distributed among several institutional actors.[76] According to the 2003 Decree, the establishment and implementation of such architecture should be based on a three-layered intervention program. The different – but interrelated – layers are: political-strategic; ministerial/administrative-tactical; procedural-operational.[77] The adoption of the National Strategic Framework and the National Plan for Cyberspace Protection represents the enactment of the required interventions at the political-strategic level. Whereas the Strategic Framework's temporal scope, intents and long-term goals are relatively broader than those outlined by the National Plan, the latter lists a set of priority measures for enhancing cybersecurity in the short/mid-term. In other words, the Plan is the roadmap to be incrementally followed for enacting

[74] Decreto del Presidente del Consiglio dei Ministri (DPCM) 27 gennaio 2014 "Strategia nazionale per la sicurezza cibernetica", in Gazzetta Ufficiale (*Official Gazette*) No. 41, 19.02.2014. The Decree adopts the "Quadro strategico nazionale per la sicurezza dello spazio cibernetico" (National Strategic Framework for Cyberspace Security), which is available both in Italian (http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf) and English (http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf). The Decree also adopts the "Piano nazionale per la protezione cibernetica e la sicurezza informatica" (National Plan for Cyberspace Protection and ICT Security), which is available both in Italian (http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/piano-nazionale-cyber.pdf) and English (http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf). 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 Italian-English equivalency, see Annex 3.

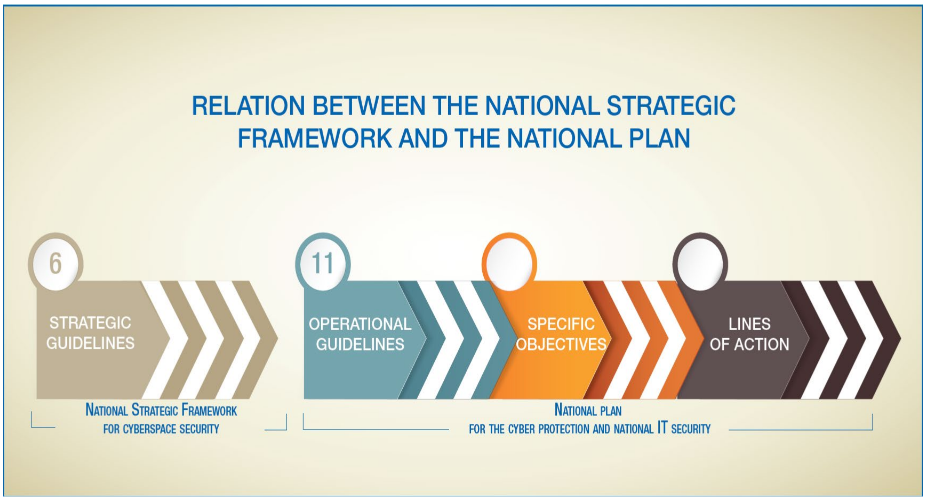
[75] Decreto del Presidente del Consiglio dei Ministri (DPCM) 24 gennaio 2013 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale", in Gazzetta Ufficiale No. 66, 19.03.2013 also available (but only in Italian) at https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2013/03/dpcm-24-01-2013.pdf. The Decree is no longer in to force because replaced by a new decree in 2017 (see infra text and footnotes).

[76] Ibid. The reduced fragmentation pursued by the Decree was coupled with the provision of mechanisms for sustaining cooperation and coordination among public and private cybersecurity players.

[77] Ibid., Preamble. The first level concerns the identification of the objectives to be pursued by the relevant institutional actors in order to promote cybersecurity in Italy, and the legislative actions that are required to achieve these objectives. The administrative and tactical layer of intervention regards the provision of permanent support to national and local administrations through the establishment of coordination mechanisms. The third level deals with crisis management *i.e.* the procedures to be activated in order to manage and respond to, and recover from, cyber-related crises.

the Framework and its declared goals. The relationship between the two policy instruments is represented by Figure ITA3 below.

Diagram ITA3: Relation between the NSF and the NP for Cyber (Source: National Plan for Cyberspace Protection and ICT Security)


RELATION BETWEEN THE NATIONAL STRATEGIC FRAMEWORK AND THE NATIONAL PLAN
6
STRATEGIC GUIDELINES
11
OPERATIONAL GUIDELINES
SPECIFIC OBJECTIVES
LINES OF ACTION
NATIONAL STRATEGIC FRAMEWORK FOR CYBERSPACE SECURITY
NATIONAL PLAN FOR THE CYBER PROTECTION AND NATIONAL IT SECURITY

By acknowledging that cybersecurity is a process rather than an end to itself, the National Strategic Framework outlines the strategy for enhancing the Country's preparedness, resilience and response to present and future challenges emerging from/through the cyberspace. The Framework provides for 6 strategic and 11 operational guidelines whose implementation requires the consistent and coordinated effort by all the actors who are part of the cybersecurity architecture at the national level. By taking into consideration the new and emerging vulnerabilities that are brought about technological innovation and the pernicious nature of cyberthreats, the National Strategic Framework sustains the adoption of defensive rather than offensive cybersecurity posture. Accordingly, it mainly endorses a reactive, resilience- and response-based approach to the protection of the Italian cyber-related interests and assets. This does not mean that prevention and anticipatory interventions are excluded from the array of options that are available to Italy for the promotion of national cybersecurity. This is quite evident from the support that the Framework and, in particular, the NP cyber give to information/intelligence gathering and analysis. The insight on actual and potential threats that is generated from these activities can be employed to run preventive interventions aimed at increasing protection.

The 11 operational guidelines identified by the National Strategic Framework are further detailed by the National Plan for Cyberspace Protection and ICT Security. The Plan represents the roadmap for the implementation of the Framework for the years 2014-2015. Each of the 11 identified operational guidelines are broken down in two several lines of actions to be implemented by the actors that are involved, at various degrees, with the promotion of cybersecurity in Italy. These are both public bodies and private organizations.

Interestingly, the implementation of the Plan's content has to be assessed periodically against an ad hoc evaluation matrix.[78]Periodic assessment and evaluation are meant as paramount procedures for identifying achievements, gaps, challenges and opportunities. Depending on their produced outcomes, further interventions can be outlined. This provides the strategy with the necessary flexibility to be re-oriented when needed.

2.1.2 The 2017 Prime Minister's Decree and the (second) National Plan for Cyberspace Protection and ICT Security

As foreseen by the 2013 Decree, the implementation of the National Plan for Cyberspace Protection and ICT Security was reviewed after about three years since its adoption.[79] The revision concerned also the whole national cybersecurity architecture as defined by the 2013 Decree. It was necessary due to both the need to keep the institutional architecture up to the evolving nature and increasing pervasiveness of cyberthreats; and the implementation of international obligations and standards in the Italian legal order. Reference is primarily made to the enactment of the

[78] Cf. Piano nazionale per la protezione cibernetica e la sicurezza informatica, p. 8. See also DPCM 24 Gennaio 2013, art. 5, par 3, letter c).

[79] Ibid.

Directive (EU) 2016/1148 on network and information security which had to be completed by May 2018 (NIS Directive).[80]

Following the revision process, the new Decree of the President of the Council of Ministers of 24 February 2017 "Guidelines for National Cyber Protection and ICT Security" was adopted.[81] The 2017 Decree, also known as "Decreto Gentiloni", re-modulates and further simplifies the Italian institutional cybersecurity architecture. It rationalizes and systematizes the responsibilities and functions of the national actors who are in charge of safeguarding national security in relation to critical infrastructures and intangible assets, with particular attention to the protection of cyber and ICT security.[82] In particular, it expands the remit of specific agencies, shortens the command chain with regard to the management of cyber-induced crises or emergencies as well as fosters cooperation mechanisms among the relevant players in cybersecurity. The publication of the new Decree was shortly followed by the adoption of the (second) National Plan for Cyberspace Protection and ICT Security.[83]

The second NP cyber confirms, updates and integrates the content of the previous Plan. It aims at boosting the implementation of the 2014 National Strategic Framework in light of the revisited national cybersecurity architecture foreseen by the 2017 Decree. In continuation to the former National Plan for Cyber, the 2017 Plan provides for 11 operational guidelines to be implemented by national stakeholders through the adoption of specific actions. Compared to the guidelines and actions provided for the 2014 Plan, there is no significant difference except for two items. These latter concern: i) the enhancement of, and better coordination among, national agencies in charge of incident prevention, response and remediation; and ii) the strengthening of intelligence, law enforcement and military functions and capabilities with regard to the cyberspace.

Notably, among the lines of action to be enacted in order to implement the guidelines, a set of interventions is given high priority. These prioritized interventions are clustered in an action plan aimed to timely put in to concrete effect the revised cybersecurity architecture, enhance the national cyber crises management system, sustain active contribution to cybersecurity from public and private actors, academia included, and stimulate cooperation among them.[84]

2.1.3 The Italian Strategy for Digital Growth 2014-2020 and Three-Year Plan for ICT in the Public Administration

Few years after the adoption of the Italian Strategy for Digital Growth 2014-2020 (also known as the Italian Digital Agenda), Italy approved the Three-Year (2017-2019) Plan for ICT in the Public Administration.[85] The two policy documents set the strategic objectives and operational guidelines for the digital transformation of the Italian central and local public administrations.[86] Although not focused on security, both instruments acknowledge that safeguarding the availability, integrity and confidentiality of information processed by the Public Administration's Information Systems is crucial for Italy. By taking in to account the goals established by the National Strategic Framework for Cyber Space Security, the Three-Year Plan emphasizes the need for rationalizing ICT-based systems and procedures employed by the Italian public administrations in order to reduce the "surface" exposed to potential cyberattacks.[87] It then

[80] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, in Official Journal L 194, 19.7.2016, p. 1–30, also available at https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG.

[81] Decreto del Presidente del Consiglio dei Ministri (DPCM) del 17 febbraio 2017 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali", in Gazzetta Ufficiale n. 87, 13.04.2017, available in Italian at http://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-17-febbraio-2017.html.

[82] Ibid., art. 1.

[83] Decreto del Presidente del Consiglio dei Ministri 31 marzo 2017 "Piano nazionale per la protezione cibernetica e la sicurezza informatica", in Gazzetta Ufficiale n. 125, 31.05.2017, available in Italian at http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf.

[84] Ibid., p. 9-12.

[85] In 2015, the Council of Ministers approved two strategic programs for the "digitalisation" of the Country: the Piano Nazionale per la Banda Ultra Larga ("National Broadband Plan"), and the Strategia per la crescita digitale 2014-2020 ("Strategy for Digital Growth 2014-2020"). The latter document is available at https://www.agid.gov.it/sites/default/files/repository_files/documenti_indirizzo/strategia_crescita_digitale_ver_def_21062016.pdf. The Piano Triennale per l'informatica nella Pubblica amministrazione 2017-2019 ("Three-Year (2017-2019) Plan for ICT in the Public Administration) was drafted by the Italian Digital Agency and then adopted by the Prime Minister on 31 May 2017. The Three Year Plan is available in Italian at https://pianotriennale-ict.italia.it/assets/pdf/Piano_Triennale_per_l_informatica_nella_Pubblica_Amministrazione.pdf. It is also available in English at https://pianotriennale-ict.readthedocs.io/en/latest/doc/01_piano-triennale-per-informatica-nella-pa.html.

[86] The Plan should be seen as a dynamic instrument, whose implementation depends on content update and transparent exchange of information with the public administrations

[87] See Piano Triennale per l'informatica nella Pubblica amministrazione, cit., Ch. 8 "Security". Cf., also Ch. 3 "Physical Infrastructures" and the planned rationalizations of communication networks, data centers, and systems for disaster recovery and business continuity.

empowers selected national agencies to take actions (assessment, enforcement, monitoring, accreditation, and supervision) to enhance the security of the networks and systems, which are used by central and local administrations.[88]

2.1.4 The 2015 White Paper on Defense

The centrality of computer networks and, in particular, the need that they remain functional, secure and resilient is also acknowledged by the 2015 White Paper on International Security and Defence.[89] The White paper was adopted by the Italian Ministry of Defence (MoD) and defines Italy's military strategic priorities and defense needs. It follows up, expands, and elaborates the guidelines contained in the Ministerial Directive on Military Policy for the Year 2013, which calls for the strengthening of operational management capabilities in the cyber spectrum.[90] It also gives further impetus to the improvements already made in the field after the adoption of the 2012 Inter-Forces Policy on Cyber Environment by the Defence General Staff.[91]

The White paper assigns to cyberdefense the general goal to safeguard the security of the Country and to strengthen the integrity of its political, economic and social institutions.[92] It accounts for the need to acquire and develop appropriate capabilities to counter cyberattacks. Such capabilities should complement those represented and deployed by national civilian agencies.[93] The above claims were reiterated by, and further elaborated in, the first and second NP cyber.[94] They were followed by two initiatives promoted by the Italian MoD that are aimed at establishing: The Joint Command for Cybernetic Operations (CIOC), which should support military operations conducted by Italy as well as favor cooperation between the Italian Armed Forces and other civilian agencies in charge of cybersecurity; [95] and the Virtual Cyber Range and Cyber-Lab. It is worth noting that the MoD has also signed a memorandum of understanding with the Italian Intelligence Agencies to better align their strategic and tactical objectives with regard to the use of cyberspace.[96]

2.2 National cybersecurity strategy: fields, tasks, priorities

The 2014 National Strategic Framework outlines the Italian cybersecurity strategy. It provides for the following 6 strategic guidelines:

1. Enhance the technical, operational, and analytical capabilities of national cybersecurity stakeholders to prevent and respond to cyberthreats;
2. Strengthen the protection of national critical infrastructures and strategic assets from cyberattacks;
3. Support public-private partnership initiatives that are aimed at safeguarding the national intellectual property and technological innovation;
4. Promote and disseminate a culture of security among individual and institutional actors and raise their cybersecurity awareness;
5. Reinforce contrast to online criminal activities in compliance with national and international law;
6. Support international cooperation in the field of cybersecurity.[97]

The six guidelines identify the main goals – and areas of intervention – pursued by Italy in order to enhance its preparedness, resilience and response to present and future cybersecurity challenges. Goals and guidelines are broad in their scope. In order to sustain their incremental achievement and implementation in the short/mid-term, they are broken down into 11 operational guidelines and further lines of actions.[98] These have been recently outlined by the

[88] Ibid, Ch. 8.

[89] Libro Bianco per la sicurezza internazionale e la difesa, available both in Italian and English at https://www.difesa.it/Content/Pagine/Libro_Bianco.aspx. The White Paper came 13 years after the last paper which was published in 2002.

[90] Ministero della Difesa, "Direttiva Ministeriale in merito alla politica militare per l'anno 2013", available also in English at https://www.difesa.it/Il_Ministro/Uffici_diretta_collaborazione/Pagine/Direttivaministeriale2013.aspx. See, p. 21, No. 78.

[91] "Direttiva di Policy Interforze sull'ambiente cibernetico", Stato Maggiore della Difesa – III Reparto "Politica Militare e Pianificazione", Centro Innovazione della Difesa (Ed. 2012). The Policy is classified.

[92] Ibid., p. 51, par 103.

[93] Ibid, p. 38, par. 68.

[94] Piano nazionale per la protezione cibernetica e la sicurezza informatica 2017, cit., Operational Guideline No. 1.

[95] Comando Interforze Operazioni Cibernetiche (CIOC). CIOC is already operational and should reach full operational capability in 2019.

[96] Piano nazionale per la protezione cibernetica e la sicurezza informatica 2017, cit., p. 12.

[97] Quadro strategico nazionale per la sicurezza dello spazio cibernetico, cit. p. 20.

[98] Cf. Ibid, p. 21-26.

second National Plan for Cyberspace Protection and ICT Security. The Plan's provisions intervene in three critical domains: State's security, meant as the capacity of national institutional actors to guarantee national security and safeguard public order; the protection of both public and private critical infrastructures; the protection of national economic interests and assets as well as community's and individual's social wellbeing and fundamental freedoms.

According to the Plan, Italy should:

1. Strengthen the intelligence and police capabilities, as well as the ones used for civil and military defense purposes;
2. Enhance the organization, coordination and cooperation among public and private cybersecurity stakeholders at the national level;
3. Promote and disseminate a culture of cybersecurity as well as sustain education and training in this field;
4. Favor international cooperation on cybersecurity and transnational exercises;
5. Implement national Computer Emergency Response Teams;
6. Foster the legislative process concerning cybersecurity, norm production, and compliance with international obligations;
7. Foster compliance with security standards and protocols;
8. Support industrial and technological development in the field of ICT and security;
9. Enhance strategic and operational communication especially during cyber-related crisis or emergencies;
10. Allocate adequate human, financial, technological and logistic resources to relevant institutional actors;
11. Define and Implement a national integrated cyber risk management system.[99]

Each of the listed operational guidelines should be enacted through the adoption and implementation of specific actions.[100] For example, the strengthening of intelligence, law enforcement and military functions and capabilities with regard to the cyberspace should be pursued through: (i) a better understanding and assessments of threats and vulnerabilities;[101] (ii) the development of cyberintelligence and knowledge management capabilities; (iii) the acquisition and development of civilian and military capabilities to contrast cyberthreats; (iv) the definition and employment of lesson-learned mechanisms.[102]

Among the several actions foreseen by the second NP cyber, eight are given high priority. These are the measures aimed at enforcing the 2017 Decree established provisions, *i.e.* enacting the new designed cybersecurity architecture and securing national assets. They intervene on the role and functions of national agencies and leverage the collaboration with private sector and academia. The eight prioritized actions consist of the following:

- Reorganization of the National Cybersecurity Unit;
- Shortening of the command and control chain for cyber crisis management;
- Simplification and rationalization of the national architecture through the unification/elimination of agencies or bodies;
- Unification of national CERTs;
- Establishment of the National Center for ICT Assessment and Certification;
- Promotion of investments in cybersecurity through venture capital or other legal institutes (foundation);
- Establishment of a National Cybersecurity Research and Development Center;
- Institution of the National Center of Cryptography.

Overall, the priority measures point to increase rapidly the level of readiness and responsiveness of the Italian cybersecurity architecture.

2.3 National cyberdefense strategy: fields, tasks, priorities

Italy does not have a stand-alone cyberdefense strategy. Cyberdefense goals are integrated into the Italian "wider" cybersecurity policy. According to the 2014 National Strategic Framework and 2017 NP cyber Italy should strengthen its cyber defense capabilities and ensure they reach and maintain high levels of efficiency and effectiveness. Capabilities should serve the primary operational purpose of protecting military networks and systems from

[99] Piano nazionale per la protezione cibernetica e la sicurezza informatica 2017, cit., p. 13-36.

[100] Ibid.

[101] In turn, this will require: a) evaluate threats and vulnerabilities on regular basis; b) monitor technological innovations in those sectors that rely on the use of ICT systems and platforms, c) share the results of threat and vulnerability assessments; d) support joint research programs on the development of innovative methodologies and tools for the early detection and analysis of threats and vulnerabilities. Ibid., p. 13-15.

[102] All the listed actions are broken down in several sub-actions. Ibid., p. 13-15.

cyberthreats.[103] They should also contribute to defend national critical infrastructures and assets from cyberattacks that may exceed the response capacity of civilian agencies. Cyberdefense capabilities should include command and control structures that are able to plan and conduct military operations in cyberspace in Italy and abroad. Again, reference is primarily made to operations aimed at achieving "defensive goals", *i.e.* protecting (actively and in-depth) Italian interests and assets from aggressive cyber-actions promoted by State and non-state actors. This is made clear several times by the 2015 White Paper on International Security and Defence. At the operational level, defense includes not only Computer Network Defense (CND) and Computer Network Exploitation (CNE), but also Computer Network Attacks (CNA) – again to achieve active and in-depth defense.[104]

Italy's pursued goals in cyber defense are in line with the objectives defined at both the NATO and EU level. Actually, enhanced cooperation at these and other bilateral levels is acknowledged as a crucial goal and it is strongly supported. Cooperation should include national and international partners and be aimed at ensuring high integration and interoperability in the planning and management process of computer network operations. It should involve the organization and participation to national and international exercises.[105]

2.4 Context/Analysis: key policy principles

The current Italian cybersecurity strategy sets out the goals, principles and guidelines that inform the actions to be taken by Italy for promoting the national cyber and ICT security. It also defines the institutional, organizational and procedural framework that should allow the country to safeguard its economic, social, scientific and industrial development as well as political and military stability from cyberthreats. The strategy is structured around broad and long-term goals which are broken down into specific mid/short-term objectives. Each objective should be pursued by national actors through the adoption and implementation of selected sets of measures. Actors range from public administration bodies, private organizations, the academia to the civil society. To note, the strategy is a *living* program, *i.e.* amenable to any necessary integration for keeping it adaptable and up to new challenges and opportunities that might stem from the cyberspace. Flexibility and adaptability are also paramount to integrate new requirements from international cooperation initiatives to which Italy is active partner.

The Italian cybersecurity policy is mainly civilian-lead and civilian-oriented. That means cybersecurity is mostly governed by civilian agencies and aims at safeguarding the Country's economic growth, social stability and national security. Nevertheless, the Italian cybersecurity policy also addresses issues pertaining to cyberdefense *i.e.* the protection, resilience and efficiency of military command and control networks as well as the acquisition and development of cyber capabilities to be deployed for military purposes.

The Italian cybersecurity policy endorses a defensive, resilience- and response-based- rather than offensive cybersecurity posture. Accordingly, it outlines a reactive/response system aimed at protecting actively and in-depth the Italian cyber-related interests and assets from cyberthreats and attacks.

The multitude of actors involved in the definition and implementation of the cybersecurity policy in Italy, demands effective coordination and efficient cooperation among these actors (see also below). The issue, which prompted the simplification and systematization of the national architecture in 2017 is still crucial.

[103] Editorial Staff, "The Joint Cyber Command is born. Interview with the Chief of Defence Staff General Claudio Graziano", in *Informazioni della Difesa*, No. 2, 2017, pp. 12-16, at https://www.difesa.it/InformazioniDellaDifesa/periodico/Periodico_2017/Documents/Numero3/ID-3_2017_ridotto.pdf.

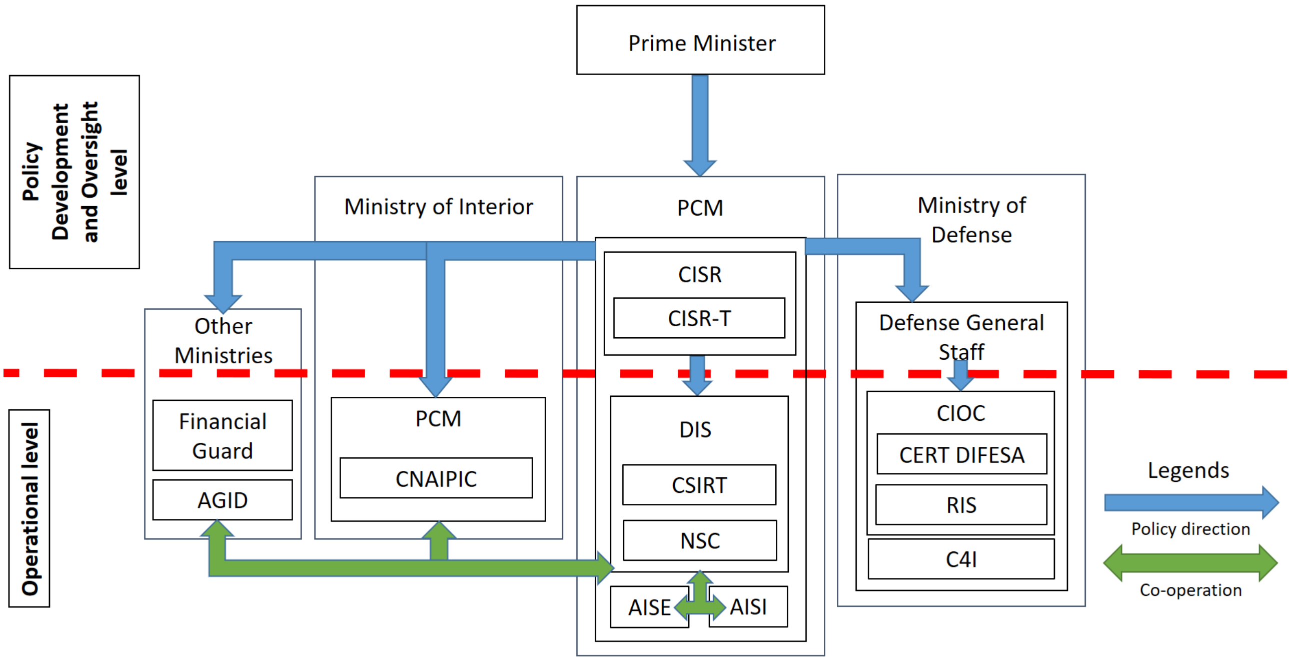
[104] Gen. B.A., F. Vestito, Cyber Commander, Joint Command for Cybernetic Operations (CIOC), "Prospettive sulla Sicurezza Cibernetica della Difesa", Presentation at Centro Studi Militari Aereonautici (CESMA), 23.01.2018, at http://www.cesmamil.org/wordpress/wp-content/uploads/2018/02/2-_-Gen.-BA-F.-Vestito-_-Propsettive-sulla-Sicurezza-Cibernetica-della-Difesa.pdf.

[105] Piano nazionale per la protezione cibernetica e la sicurezza informatica 2017, cit., p. 20.

3. Current public cybersecurity structures and initiatives

3.1 Overview of national organization framework

Diagram ITA4: Oversight organization



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

3.2.1 The National Cybersecurity Architecture: Key Players

In Italy, the implementation of the cybersecurity policy relies on the active contribution of several governmental agencies, private organizations and the academia, who overall compose the Italian cybersecurity architecture. From an organizational perspective, the strategic leadership of, and ultimate responsibility for, all aspects of cybersecurity lies with the Prime Minister who exercises it through structures and functions established within the Presidency of the Council of Ministers. The Prime Minister approves the Italian cybersecurity strategy and promotes its practical implementation trough the adoption of specific directives. The Prime Minister's decision-making process is supported by the Inter-ministerial Committee for the Security of the Republic (CISR), a collegial organ that has advisory and consultancy role, also during cyber crises or emergencies.[106] In particular, the CISR can propose the Prime Minister the adoption of specific legislation, policies, directives and measures aimed at strengthening the national cybersecurity as well as promote the coordinated participation of Italy to cybersecurity-related initiatives at the international level.[107] The CISR sets also the requirements related to the promotion of the domestic cybersecurity to the national intelligence agencies.[108] Technical Assistance to the activities of the CISR is provided by the Inter-ministerial Committee for the Security of the Republic "at the working level" ("CISR tecnico") who is also in charge of verifying and monitoring the implementation of the National plans for Cyberspace Protection and ICT Security (see above).[109]

The Department of Information Security (DIS) plays a central role with regard to the promotion of cybersecurity in Italy. Together with its coordinated agencies (AISE and AISI), it contributes to the intelligence function for the Italian

[106] Comitato Interministeriale per la Sicurezza della Repubblica. The CISR is chaired by the President of the Council of Minister and includes: Delegated Authority (an appointed Undersecretary of State or Minister without portfolio), Minister of Foreign Affairs, Minister of the Interior, Minister of Defense, Minister of Justice, Minister of Economy and Finance, Minister for Economic Development, The Director General of the DIS acts as the Committee's secretary.

[107] Decreto del Presidente del Consiglio dei Ministri (DPCM) del 17 febbraio 2017, cit. art. 4.

[108] Ibid.

[109] Ibid, art. 5. Organismo di supporto al CISR, "CISR tecnico".

decision and policy makers.[110] The DIS coordinates the gathering of relevant information and all-source intelligence on cyberthreats, produces strategic analysis, assessments and forecasts, and favors intelligence sharing among public agencies and administrations, and the private sector. It promotes awareness-raising campaigns and educational initiatives in the field of cybersecurity.[111] Within the DIS, there is the Cybersecurity Unit who is in charge of cyber crises management (see below). Following the entry in to force in June 2018 of the Legislative Decree n. 65, which implements the provisions of the EU Directive 2016/1148 (NIS Directive), the DIS will assume the role of national single point of contact responsible for coordinating issues related to the security of network and information systems and cross-border cooperation at the European Union level.[112]

It is worth noting that the Prime Minister, the CIRS, the DIS, AISI and AISE integrate collectively what is generally known as the Intelligence System for the Security of the Republic (Security Intelligence System).[113] In light of what described above, all the System's components have a significant stake with regard to cybersecurity. In other words, cybersecurity falls predominately within the scope on the System's remit. This makes sense given that the organizations integrating the System have the overall goal to protect Italy's political, military, economic, scientific and industrial interests; and cybersecurity-related issues might affect any of these interests.

The implementation of the cybersecurity policies is also demanded to different Ministries who have a stake into that. These are the same ministries represented in the CISR. For example, the Ministry of Foreign Affairs ensures the promotion and safeguard of national interests with regard to cybersecurity in different international fora and organizations. The Ministry of Interior is in charge of the prevention and contrast of cybercrime and the terroristic use of the Internet. On an operative level, the Postal and Communication Police pursues cyber and internet-related illegal activities. It runs the National Anti-Crime Computer Center for the Protection of Critical Infrastructures (CNAIPIC) that is responsible for countering attacks against critical infrastructures or ICT assets of national relevance. The Ministry of Economic Development is responsible for regulating the security and integrity of electronic communication systems. It also operates the National Computer Emergency Response Team (CERT-N). The Ministry of Finance is in charge of the integrity of various national Critical computer infrastructures and acts through the financial police to pursue financial and economic frauds via the Internet. The Italian Digital Agency (AGID) is responsible for implementing the provisions of the Italian Digital Agenda which concern the digitalization of public administration's provided services. The AGID operates the Computer Emergency Response Team for the Public Administration (CERT-PA).

Following the entry in to force in June 2018 of the Legislative Decree n. 65, the responsibilities and tasks of the CERT-N and CERT-PA will be assumed by the CSIRT (starting from November 2018). The CSIRT will be established within the Presidency of the Council of Ministers.[114]

The above-described national cybersecurity architecture includes also representatives from private sector organizations and the academia. The former's contribution is framed within a public-private partnership (see also below). With regard to academia, it supports national cybersecurity with research, training and educational programs. It is worth mentioning the active participation of the National Laboratory of Cybersecurity to the national policy agenda setting.[115]

3.2.2 Cyber crisis management: The Cybersecurity UNIT (NSC)

The Department of Information Security includes the Cybersecurity Unit (NSC).[116] Originally established within the Prime Minister Military Advisor's Office, the Unit was re-positioned within the DIS by the 2017 Decree. The NSC is a

[110] The Agenzia Informazioni e Sicurezza Esterna (AISE, External Intelligence and Security Agency) is responsible for safeguarding national security against threats originating abroad. The Agenzia Informazioni e Sicurezza Interna AISI (Internal Intelligence and Security Agency) is responsible for safeguarding national security from threats originating within Italy's borders. Both AISE and AISI have the mandate of protecting Italy's political, military, economic, scientific and industrial interests.

[111] Decreto del Presidente del Consiglio dei Ministri (DPCM) del 17 febbraio 2017, cit. art. 7.

[112] Decreto Legislativo n. 65, 18 maggio 2018 "Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione", in Gazzetta Ufficiale No. 132, 9.06.2018 also available (but only in Italian) at http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/06/Dlgs-65_2018-NIS.pdf. For more details see also http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/cyber-la-nis-entra-in-vigore-litalia-si-rafforza-e-fa-rete-con-lue.html

[113] Sistema di informazione per la Sicurezza della Repubblica. The Intelligence System can also include a Delegated Authority when this latter is appointed by the Prime Minister. For further information see (in English) http://www.sicurezzanazionale.gov.it/sisr.nsf/english.html.

[114] See also https://www.csirt-ita.it/.

[115] The Laboratory is a multidisciplinary organisms consisting of representatives from several public Universities and Research Centers across Italy. It is established within the National Interuniversity Consortium for Informatics (CINI), which promotes and coordinates scientific activities of research and technological transfer, both basic and applicative, in several fields of Computer Science and Computer Engineering. In 2015 and 2017, the Laboratory drafted "The White Book on Cybersecurity", which describes the main challenges, and opportunities Italy faces in this sector. For more information on the Laboratory and its activities, see https://www.consorzio-cini.it/index.php/en/labcs-home/labcs-mission.

[116] Nucleo per la Sicurezza Cibernetica, Ibid., art. 8

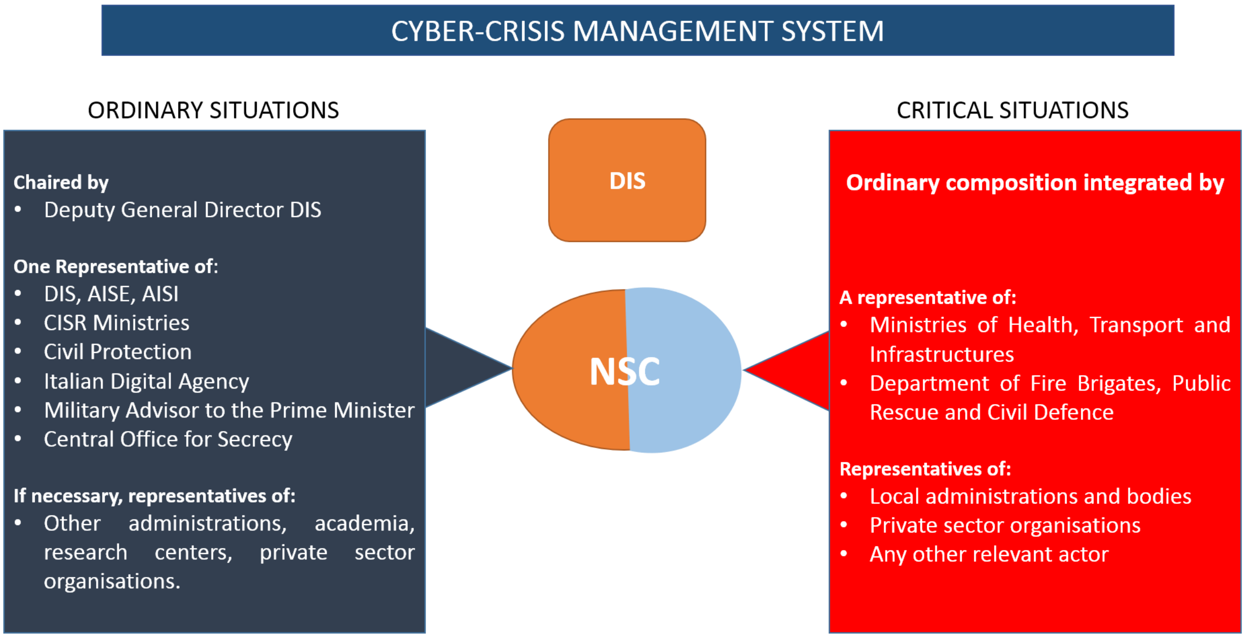
permanent collegial organ that is chaired by one Deputy General Director of the Department. It deals with preparedness to, prevention of, response to, and recovery from cyber-related crisis. It is the focal point with regard to cyber crises operational management (*ex-ante*, in, *ex-post*) and serves as connector and coordinating entity among the several institutions, agencies and organizations who define and contribute to the national cybersecurity architecture. Its compositions varies depending on whether a cyber-related "ordinary" incident evolves into or generates a "state of crisis" (see Figure ITA5).

The NSC is in charge of:

- Programming and planning the operational response to crises;
- Running the early warning and response unit on a 24/7/365 basis;
- Assessing and promoting the adoption of information sharing procedures to be implemented in case of a crisis;
- Gathering and conveying communication on cyberthreats and/or attacks against national networks, systems and infrastructures;
- Promoting exercises at the national and international level;
- Liaising with international actors like UN, NATO, UE or other States;
- Collecting and distributing alerts provided by both national and international agencies;
- Assessing the nature and reach of an event and deciding whether it integrates a crisis.

In the event of a cyber crisis, the NSC should ensure the coordinated response of national administrations and other involved actors. For the very technical response, it can rely on the support and activities of the Computer Emergency Response Teams (CERTs), in particular the national-CERT (set within the Ministry of Economic Development) and the CERT-PA (set within the Italian Digital Agency) – to be fused in the Italian CSIRT from November 2018 (see above). Further to coordinating the actions and intervention of national actors for handling cyber-incidents and restoring network functionality, the NSC acts as point of contact with NATO, the European Union, and other international organizations during a crisis.[117]

Diagram ITA5: The Cyber-Crisis Management System. (Source: Re-elaboration of diagram reproduced in Relazione sulla Politica dell'Informazione per la Sicurezza, 2017)


CYBER-CRISIS MANAGEMENT SYSTEM

ORDINARY SITUATIONS

Chaired by
- Deputy General Director DIS

One Representative of:
- DIS, AISE, AISI
- CISR Ministries
- Civil Protection
- Italian Digital Agency
- Military Advisor to the Prime Minister
- Central Office for Secrecy

If necessary, representatives of:
- Other administrations, academia, research centers, private sector organisations.

CRITICAL SITUATIONS

Ordinary composition integrated by

A representative of:
- Ministries of Health, Transport and Infrastructures
- Department of Fire Brigates, Public Rescue and Civil Defence

Representatives of:
- Local administrations and bodies
- Private sector organisations
- Any other relevant actor

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

As participant to the CISR, the Ministry of Defence contributes to the policy-making and implementation processes with regard to cybersecurity. Through its dedicated structures and functions, it adopts and implements the

[117] Ibid. art. 10.

measures that are aimed at countering potential or actual threats to military or other critical networks, computer systems and services on the national territory or in-theater.[118]

Within the MoD, the Defence General Staff is the highest military authority that coordinates and supervises the various sectors of activities in the technical-operational area of Defence, cyberdefense included. In particular, cyberdefense is the remit of two different divisions of the Defence General Staff: the II° "Information and Security" and the IV° "Command, Control, Communication, Computer and Information Systems" (C4I) Divisions. Each of them oversees specific functions of the CERT of the Italian Armed Forces (CERT DIFESA), which is in charge of safeguarding the Armed Forces' computer systems and networks from malicious activities at the operational level.

The CERT DIFESA consists of two structures. The "Coordination Centre" that is part of the II° Division. It coordinates the sharing of information among the CERTs established within each Armed Forces (Navy, Air Force, Army, Carabinieri) as well as it liaises with civilian CERTs at both the national and international level. The second structure is the "Technical Center" that operates under the IV Division "Command, Control, Communication, Computer and Information Systems" (C4I). It provides technical and specialized assistance on cyber-related issues to the Armed Forces.

The above-described framework has been recently integrated with the Joint Command for Cyber Operations (CIOC). Envisaged in the 2015 "White Paper on International Security and Defense", the CIOC has achieved initial operational capacity in September 2017.[119] Together with the military CERTs, CIOC contributes to the protection of military assets and installations. It is also in charge of planning and conducting "cyber-operations" both in Italy and, if required, abroad. The CIOC will rely on specialized staff and technical equipment capable of supporting the Command activities. As per the staff, it will benefit from special education and training provided through facilities like the Cyber Range, and the virtual Cyber-Lab – to be also employed for keeping personnel's operational readiness.[120] The CIOC can also deploy Cyber Operative Cells (COC) among the forces projected in operational theaters.

3.4 Context: key public organizational framework

The Italian institutional framework governing cybersecurity is a hybrid version between a centralized and decentralized/distributed model. It relies on the active participation of several governmental agencies, private organizations and the academia, who overall compose the Italian cybersecurity architecture. The strategic leadership of, and ultimate responsibility for, all aspects of cybersecurity lies with the Prime Minister who exercises it through structures and functions established within the Presidency of the Council of Ministers, in particular, via the Department of Information Security. Other Ministries – in particular, the Home Affairs, Economic Development, Defence, Foreign Affairs, Justice, and Economy – and administrations have a significant stake in the definition and implementation of the cybersecurity policy, and actively support the Prime Minister's strategic direction.

Due to the multitude of actors composing the cybersecurity architecture – at the vertical (national, regional, local) and horizontal (civilian and military; public and private sector) level –, coordination and cooperation among these actors remains crucial to the definition and efficient implementation of policies and measures. The Italian legislator considered these aspects when it enacted the 2017 rationalization of the Italian cybersecurity framework.[121] At the strategic-political level, coordination among ministries and administrations is ensured by the participation of their representatives to the Inter-ministerial Committee for the Security of the Republic (CISR). At the tactical-operational level, coordination is tasked to the DIS and its NSC, which connect the several institutions, agencies and organizations (private sector and academia included) integrating the cyber crisis management system. With regard to intelligence collection on cyber-related issues, a memorandum of understanding between the Italian Intelligence Agencies and the military information structures fosters harmonized collaboration in the area. For the technical response, the NSC can rely on the to-be-established national CSIRT, which will ensure liaising with the different CERTs established within the Italian jurisdiction (public administration and private sector). At the international level, the NSC will be also responsible for coordination and cross-border cooperation with the NATO, the European Union and other international actors. The above setting should limit potential overlapping, duplications or contradictions among the measures and actions that are taken by the relevant cybersecurity stakeholders.[122] It should favor a harmonized and consistent response to cyber-menaces and attacks.

[118] Cf. http://www.esercito.difesa.it/Rapporto-Esercito/Documents/2017/CYBER%20DEFENCE.pdf (in Italian).

[119] Final operational capability is expected to be achieved within 2019. For further info see, F. Vestito, "The Italian Cyber Defence Build-Up", in ISPI Commentary, May 2, 2018, at https://www.ispionline.it/sites/default/files/pubblicazioni/commentary_vestito_02.05.2018.pdf.

[120] Ibid. The Cyber Range and Cyber-Lab will collaborate with the NATO Cooperative Cyber Defence Center of Excellence - CCD COE - in Tallinn) and work in full synergy with the academic and industrial world.

[121] See Section 2.1.2 above.

[122] Some frictions may anyhow arise but these should be solved within the above-identified fora in a spirit of mutual institutional collaboration.

As already discussed, in Italy cybersecurity is mainly civilian-lead and civilian-oriented. This is made evident by the described architecture who has civilian institutions and agencies (Prime Minister, CISR, DIS, CSIRT) playing core roles in the field.[123] The same institutions and agencies that integrate the Intelligence System for the Security of the Republic. This is not trivial. It confirms the institutional view about cybersecurity as a policy area that has multifaceted aspects and impacts on the integrity, security, stability, sovereignty, economic and social prosperity of the Nation. Converging cybersecurity around the Intelligence System is in line with the latter's overall mandate to protect Italy's political, military, economic, scientific and industrial interests. To note that the weighting towards civilian guidance and oversight has been further increased with the relocation of the NSC from the Prime Minister Military Advisor's Office to the DIS in 2017. The relocation responded to the practical need of rationalizing the command and control chain with regard to the management of cyber-induced crises or emergencies. It is also consistent with the institutional view mentioned above.

Relevant components of the cybersecurity architecture are the MoD and its military structures, which contribute to safeguard Italy against cyberthreats that may jeopardize the integrity of its political, economic and social institutions. In particular, they are responsible for securing military networks and systems as well supporting military operations in cyberspace for defense purposes. They also concur to defend national critical infrastructures and assets from cyberattacks that may exceed the response capacity of civilian agencies. From this perspective, they complement civilian institutions when necessary. In terms of capabilities, the establishment of the Joint Command for Cyber Operations, the Cyber Range and Virtual Cyber-Lab aims at enhancing the ability of the Country to respond to cyberattacks. It aligns Italy with other Countries which have set up (or are creating) similar structures.[124] As per the Joint Command for Cyber Operations is concerned, it will be entitled to plan and engage in Computer Network Defense, Computer Network Exploitation, and Computer Network Attacks. However, the establishment of the CIOC is probably triggering a process of internal harmonization of cyberdefense competencies, which are now distributed also with the II° and VI° Division of the Defence General Staff.

[123] See *supra*.

[124] F. Vestito, The Italian Cyber Defence Build-Up, cit. Cf. also https://www.difesaesicurezza.com/difesa-e-sicurezza/le-risposte-presenti-e-future-della-difesa-italiana-alle-cyber-minacce/.

4. Cyberdefense and Cybersecurity partnership structures and initiatives

4.1 Public-Private cyberdefense partnerships

The Italian cybersecurity policy strongly supports public-private partnership initiatives that are aimed at promoting the national interests in and through the cyberspace, and safeguarding the Country's critical assets. Overall, the partnership entails: collaboration (*e.g*. info-sharing, exercises, notifications of security breaches) and coordination (*e.g.* joint working groups) among public and private organizations, especially those providing services which are essential for the maintenance of critical societal and/or economic activities; promotion of industrial and technological development in the field of ICT security (*e.g.* through venture capital or star-up financing schemes). With regard to cyberdefense, there are not detailed information on *ad hoc* partnerships between the MoD and the private sector.

4.2 International cyberdefense partnerships

At the international and regional level, Italy favors cooperation on cybersecurity with the UN, G7, NATO, OSCE and the EU. With regard to cyberdefense, Italy participates regularly to NATO promoted initiatives and collaborates with the Cooperative Cyber Defence Center of Excellence (CCDCOE) based in Tallinn. For example, Italy fully supported the Cyber Defence Pledge made by NATO allies after the Warsaw Summit in 2016.[125]The CERT DIFESA Coordination Centre interacts with the NATO Computer Incident Response Capability (NCIRC) and participates in the annual NATO Cyber Coalition Exercises, which are organized to encourage communication between NATO structures and the CERTs of the Armed Forces in case of cyber crisis.

Through the structure and functions of the MoD and the Ministry of Foreign Affairs, Italy also contributes to initiatives concerning cyberdefense that are promoted within the EU. It collaborates with the European Defence Agency (EDA) as well as the EU Military Staff (EUMS).[126].

4.3 Cyberdefense awareness programs

Throughout the Italian current cybersecurity policy there are several awareness-raising programs and campaigns targeted at various sectors of society. There is, however, little specific detail provided regarding cyberdefense awareness campaigns.

4.4 Cyberdefense education and training programs

The Italian MoD is giving particular emphasis to the need to educate and train its (newly recruited or existent) staff with regard to cybersecurity-related issues. Further to informative campaigns offered to the whole personnel (civilian and military), the MoD is sustaining *ad hoc* training and formative programs that address the staff working in those structures and services in charge of cyberdefense. Programs aim at building highly specialized staff, which is able to operate with technical equipment according to established operational procedures. Staff – part of which to be recruited from Universities, research centers or other civilian organizations – will benefit from special education and training programs provided through facilities like the Cyber Range, and the virtual Cyber-Lab. These latter will be also employed for keeping personnel's operational readiness. To test and improve staff' skills, the MoD also organizes or takes part to annual exercises on cyberdefense, at both the national or international level.

4.5 Cyberdefense research programs

Throughout the Italian current cybersecurity policy documents, cybersecurity-related research (technical capabilities) is actively promoted in the National Plan for Cyber Security (NP cyber 2017), which has notably called for the establishment of a National Cybersecurity Research and Development Center.

[125] For more information, see https://www.nato.int/cps/en/natohq/topics_78170.htm.

[126] The EU Military Staff and the European Defence Agency are working to improve the EU cyber defense capabilities. Given that the EU does not have standing military forces or EU- owned military equipment, it relies on member States capabilities.

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 ITA6: Spectrum of Centralization vs Decentralization of policy development and management

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

5.2 Civilian vs defense posture and oversight

Diagram ITA7: Spectrum of Civilian-Defense cybersecurity posture and oversight

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

5.3 Offensive vs defensive capabilities

Diagram ITA8: Spectrum of Offensive vs Defensive cyberdefense capabilities

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

6. Annex 2: Key definitions

Term	Definition
Cyber crisis (DPCM 17.02.2017, art. 2)	Extraordinary situation when the extension, reach and nature of a cyber-related event impact on the national security and requires the coordinated intervention of different administrations at the ministerial level
Cyberdefense (Glossario Intelligence)	The whole doctrine, organizational settings, and activities aimed at prevent, detect, limit and contrast the consequences of attacks run in, through or against the cyberspace and its fundamental elements.
Cyberintelligence (Glossario Intelligence)	Research and analysis of relevant information within or regarding the cyberspace in order to prevent, detect, contain and contrast threats to national security, for example, to critical infrastructures
Cybersecurity (DPCM 17.02.2017, art. 2)	Security of the cyberspace to be achieved through the adoption of adequate physical, logical and procedural measures aimed at protecting it from accidental or malicious events. These events can consists in the unlawful collection, transferring, modification, cancellation of data, or illegitimate control, disruption, damage, interference with the normal functioning of information systems and networks and their fundamental elements (cf. also cyberthreat definition)
Cyberspace (DPCM 17.02.2017, art. 2)	Complex of interconnected information and communication infrastructures, including hardware, software, data, users as well as the logical connections established among them
Cyberthreat (DPCM 17.02.2017, art. 2)	Complex of malicious conducts that can be executed in, through or against the cyberspace and its fundamental elements. These conducts may consists in actions perpetrated by individuals or organizations (State, non-State, public or private) that are aimed at unlawfully collecting, transferring, modifying, cancelling data, or illegitimately controlling, disrupting, damaging, interfering with the normal functioning of information systems and networks and their fundamental elements

7. Annex 3: Abbreviations

Abbreviation	English	Italian
AISE	External Intelligence and Security Agency	Agenzia Informazioni e Sicurezza Esterna
AISI	Internal Intelligence and Security Agency	Agenzia Informazioni e Sicurezza Interna
AGID	Italian Digital agency	Agenzia per l'Italia digitale
C4I	C4 division	Comando C4 Difesa
CERT DIFESA	Computer Emergency Response Team for the Armed Forces	Computer Emergency Response Team per le Forze Armate
CERT-N	National Computer Emergency Response Team	Computer Emergency Response Team Nazionale
CERT-PA	Computer Emergency Response Team for the Public Administration	Computer Emergency Response Team per la Pubblica Amministrazione
CIOC	Joint Command for Cybernetic Operations	Comando Interforze Operazioni Cibernetiche
CISR	Committee for the Security of the Republic	Comitato Interministeriale per la Sicurezza della Repubblica
CISR-T	Committee for the Security of the Republic – technical	Comitato Interministeriale per la Sicurezza della Repubblica - Technico
CNAIPIC	National Anti-Crime Computer Center for the Protection of Critical Infrastructures	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
CSIRT	Computer Security Incident Response Team	
DIS	Department of Information Security	Dipartimento delle Informazioni per la Sicurezza
DPCM	Decree of the President of the Council of Ministers	Decreto del Presidente del Consiglio dei Ministri
ICT	Information and Communication Technology	Tecnologia per la Comunicazione e Informazione
MoD	Ministry of Defence	Ministero della Difesa
NP cyber	National Plan for Cyberspace Protection and ICT Security	Piano nazionale per la protezione cibernetica e la sicurezza informatica
NSC	Cybersecurity Unit	Nucleo per la Sicurezza Cibernetica
NSF	National Strategic Framework for Cyberspace Security	Quadro strategico nazionale per la sicurezza dello spazio cibernetico
PCM	Office of the Prime Minister.	Presidenza del Consiglio dei ministri
PCP	Postal and Communication Police	Polizia Postale e delle Comunicazioni
RIS	Information and security division	Reparto Informazioni e Sicurezza

8. Bibliography

Editorial Staff, “The Joint Cyber Command is born. Interview with the Chief of Defence Staff General Claudio Graziano”, in Informazioni della Difesa, No. 2, 2017, pp. 12-16, at https://www.difesa.it/InformazioniDellaDifesa/periodico/Periodico_2017/Documents/Numero3/ID-3_2017_ridotto.pdf.

F. Vestito, “Prospettive sulla Sicurezza Cibernetica della Difesa”, Presentation at Centro Studi Militari Aereonautici (CESMA), 23.01.2018, at http://www.cesmamil.org/wordpress/wp-content/uploads/2018/02/2-_-Gen.-BA-F.-Vestito-_-Propsettive-sulla-Sicurezza-Cibernetica-della-Difesa.pdf.

F. Vestito, “The Italian Cyber Defence Build-Up”, in ISPI Commentary, May 2, 2018, at https://www.ispionline.it/sites/default/files/pubblicazioni/commentary_vestito_02.05.2018.pdf.

The Netherlands

Raymond Bierens
University of Amsterdam
Nicolas Castellon
Dcypher

Highlights/Summary:

1. Key national trends

The Netherlands is proactive regional and international actor in the field of ICT. Due to the presence of important digital infrastructures (e.g. the Amsterdam Internet Exchange) and being one of the most ICT-intensive economies in Europe, the Netherlands ambitions to be a digital and cybersecurity leader. Policy wise, awareness on the issue particularly rose after various national and international cyber-incidents, which have led the Dutch government to adopt a risk-based approach to improve both resilience of CI and reinforce public-private/civilian-military collaboration.

2. Key policy principles

2.1 Cybersecurity

The Dutch cybersecurity approach is holistic, comprehensive and inclusive. The strategy endorses fostering the cyber resilience, preparedness, awareness and privacy of the all members of society. As such, its policies include critical information infrastructure protection, national and international cybercrime prevention, cyber diplomacy, the enhancement of civil-military cooperation and the promotion of innovation and expertise.

2.2 Cyberdefense

The second iteration of the Dutch Cyberdefense strategy focuses mainly on defensive measures, such as improving robustness and resilience of its own information infrastructure as well as developing its situational threat awareness. In addition, the Ministry of Defence (MoD) is to invest in capabilities to “keep the preponderance in the context of military operations” (Ministry of Defence, 2018).

3. Key national framework

3.1 Cybersecurity

Currently, there is in the Netherlands no single agency with an overarching authority to ensure the national cybersecurity architecture is achieved. The civilian government leads the policy-strategic dimension, with the support of and hybrid body (i.e. the Cyber Security Council), while the operational responsibilities are decentralized to the respective ministries, agencies and actors (over 20 different entities) with particular areas of expertise. Specifically, the leading agencies are split between the ministry of security and justice (e.g. National Cybersecurity Center) and the ministry of Economic affairs and climate (e.g. Digital trust center).

3.2 Cyberdefense

The Dutch cyberdefense posture is that of active defense. Accordingly, most of the capabilities and responsibilities are centralized within the Defense Cyber Command and its operational arm the DefCERT. The different military entities nonetheless collaborate with their civilian counterparts in terms of situational picture through a joint SIGINT cyberunit. In addition, a cyber reservist program has recently been set up.

4. Level of partnership and resources

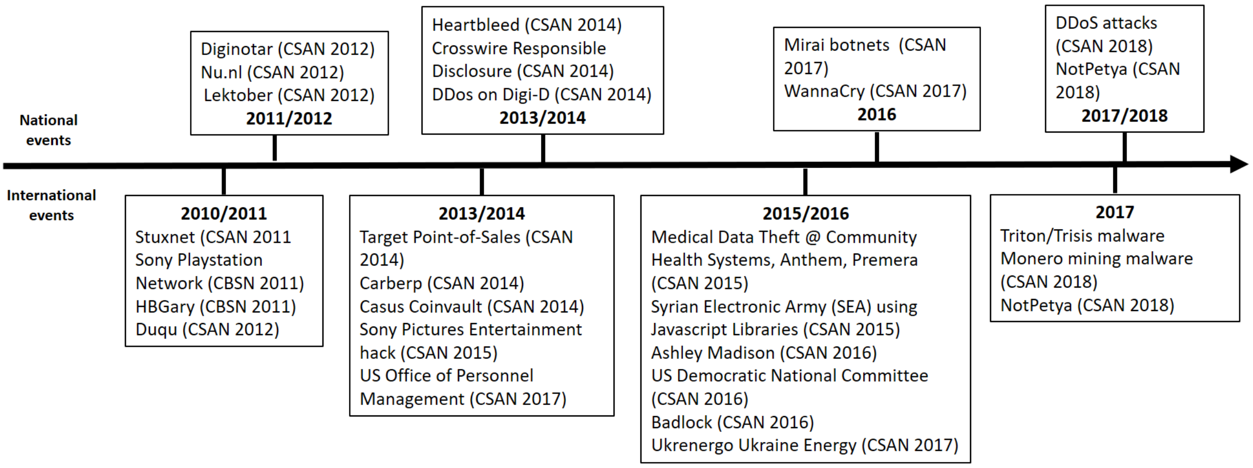
The Netherlands actively cooperates on cybersecurity issues (e.g. research, education, exercise) with its allies within NATO (e.g. CCDCOE) and the EU. In addition, it actively promotes the private sector’s involvement in cybersecurity policy making, research and awareness-raising, notably through the Cyber Security Council or public-private partnerships (e.g. the Cyber Security Alliance).

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

1.2 Threat perception: trigger events

As outlined in the first Dutch National Cyber Security Strategy, the National Coordinator for Security and Counterterrorism releases the Cyber Security Assessment Netherlands (CSAN) that offers insight into threats, interests and resilience in the field of cybersecurity in relation to national security. The CSAN is published annually and is written in close cooperation with public and private partners. Each CSAN contains national and international events that have triggered the development of digital and cybersecurity policies. Diagram 1 below shows the major triggers that have been referenced in the CSAN from 2011 until 2018. The arrows indicate the triggers causing the major effect in The Netherlands).

Diagram NL1: Timeline of Trigger events



National events

Diginotar (CSAN 2012)
Nu.nl (CSAN 2012)
Lektober (CSAN 2012)
2011/2012

Heartbleed (CSAN 2014)
Crosswire Responsible Disclosure (CSAN 2014)
DDos on Digi-D (CSAN 2014)
2013/2014

Mirai botnets (CSAN 2017)
WannaCry (CSAN 2017)
2016

DDoS attacks (CSAN 2018)
NotPetya (CSAN 2018)
2017/2018

International events

2010/2011
Stuxnet (CSAN 2011
Sony Playstation Network (CBSN 2011)
HBGary (CBSN 2011)
Duqu (CSAN 2012)

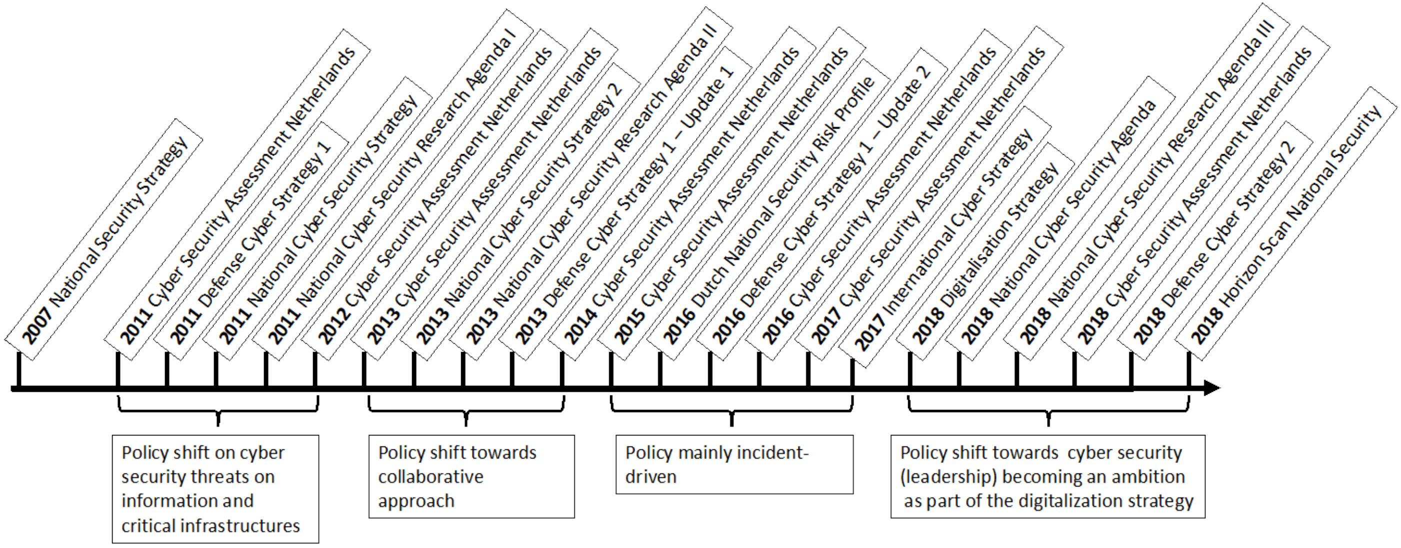
2013/2014
Target Point-of-Sales (CSAN 2014)
Carberp (CSAN 2014)
Casus Coinvault (CSAN 2014)
Sony Pictures Entertainment hack (CSAN 2015)
US Office of Personnel Management (CSAN 2017)

2015/2016
Medical Data Theft @ Community Health Systems, Anthem, Premera (CSAN 2015)
Syrian Electronic Army (SEA) using Javascript Libraries (CSAN 2015)
Ashley Madison (CSAN 2016)
US Democratic National Committee (CSAN 2016)
Badlock (CSAN 2016)
Ukrenergo Ukraine Energy (CSAN 2017)

2017
Triton/Trisis malware
Monero mining malware (CSAN 2018)
NotPetya (CSAN 2018)

1.2 Main Policy Documents: Key Shifts in Strategy

Diagram NL2: Timeline of Policy Events and Trends



2007 National Security Strategy
2011 Cyber Security Assessment Netherlands
2011 Defense Cyber Strategy 1
2011 National Cyber Security Strategy
2011 National Cyber Security Research Agenda I
2012 Cyber Security Assessment Netherlands
2013 Cyber Security Assessment Netherlands
2013 National Cyber Security Strategy 2
2013 National Cyber Security Research Agenda II
2013 Defense Cyber Strategy 1 – Update 1
2014 Cyber Security Assessment Netherlands
2015 Cyber Security Assessment Netherlands
2016 Dutch National Security Risk Profile
2016 Defense Cyber Strategy 1 – Update 2
2016 Cyber Security Assessment Netherlands
2017 Cyber Security Assessment Netherlands
2017 International Cyber Strategy
2018 Digitalisation Strategy
2018 National Cyber Security Agenda
2018 National Cyber Security Research Agenda III
2018 Cyber Security Assessment Netherlands
2018 Defense Cyber Strategy 2
2018 Horizon Scan National Security

Policy shift on cyber security threats on information and critical infrastructures

Policy shift towards collaborative approach

Policy mainly incident-driven

Policy shift towards cyber security (leadership) becoming an ambition as part of the digitalization strategy

1.3 Organizational structures: key parameters

The Dutch national cybersecurity landscape is highly decentralized with the majority of activities being carried out by the Ministry of Justice and Security, Ministry of Economic Affairs & Climate, and military efforts carried out by the Cyber Command of the Ministry of Defence. The Ministry of Justice and Security is the host institution to the National Cyber Security Centre (NCSC-NL), the organization tasked to ensure the cybersecurity of the Central Government and the Dutch Critical National Infrastructure (CNI) organizations. Responsibility for cybersecurity does not solely rest with the Ministry of Justice and Security. This ministry and the NCTV is responsible for coordinating interdepartmental cybersecurity efforts between various civilian and military units that have cybersecurity responsibilities. The NCTV also oversees most of the cybersecurity-related initiatives occurring in the Netherlands, however, given the decentralized governance, the Ministry of Justice and Security does not have the responsibility nor the mandate to direct the activities of other Ministries, such as the Ministries of Interior and Kingdom Relations, Economic Affairs and Climate; Defense, Foreign Affairs, and Education, Culture and Science; and other governmental agencies like the National Police, and the Intelligence and Security Agencies. In regard to the military, the Cyber Command is tasked for overseeing the cyberdefense of the Netherlands in regard to foreign threat actors.

The second National Cyber Security Strategy (NCSS 2) identified the individual and collective responsibilities of the organizations involved in achieving its cybersecurity objectives. On the government side, these include the Dutch Ministry of Justice and Security that is also responsible for coordinating interdepartmental cybersecurity efforts between various civilian and military units that have cybersecurity responsibilities, including the Ministries of Interior and Kingdom Relations, Economic Affairs and Climate; Defense, Foreign Affairs, and Education, Culture and Science; and other governmental agencies like the National Police, and the Intelligence and Security Agencies.

Academia is also involved via the Dutch Research Council (Nederlandse Organisatie voor Wetenschappelijk Onderzoek, NWO) and through government financing of independent research organizations.

1.4 Context/Analysis: key national trends

The Netherlands has positioned itself as an important regional and international actor. Since its presidency of the European Union during the first half of 2016, the Netherlands has increased its role as an important player in European affairs and the European Union. The Netherlands also takes active part in the United Nations, the Organisation of Economic Cooperation and Development, the European Union and NATO. Geographically positioned between the United Kingdom and Germany, The Netherlands has traditionally articulated its foreign policy around three main topics: Europe, International Trade and the transatlantic partnership – the latter incentivized through participating to the NATO cooperation framework. As a member of the European Union, the Netherlands contributes to shaping the EU policies and initiatives in many areas.

The Netherlands considers itself a global leader in digitalization due to the presence of the largest internet hubs in the world, the Amsterdam Internet Exchange (AMS-IX), the NL-IX and many data centers, but also its various lightning-fast, broadband telecom networks. This makes The Netherlands one of the most ICT-intensive economies in Europe. In addition to Schiphol and the port of Rotterdam, the Dutch digital infrastructure has become the third main port of our country. Due to its two internet hubs, the Netherland also has the most direct connections to the US and will be in a similar position towards the UK depending on how the Brexit process will unfold.

As the Netherlands is a forerunner in digitization, they are one of the first countries to encounter its adverse effects. The Dutch Government therefore committed to a structural investment of 95 million euro for cybersecurity. The Dutch Government takes a risk-based approach to increase the resilience of critical national infrastructure services and processes, and work to an effective joint public-private and civil-military response. Triggered by the Diginotar incident in 2012, the primary focus was on cybersecurity threats on information and CNI. The Ddos on Digi-D and Heartbleed created the awareness that a collaborative with (inter)national partners was necessary to mitigate risks. This partnership maintained throughout the next years until 2018 marked the shift towards cybersecurity leadership becoming an ambition in alignment with the newly released digitalization strategy.

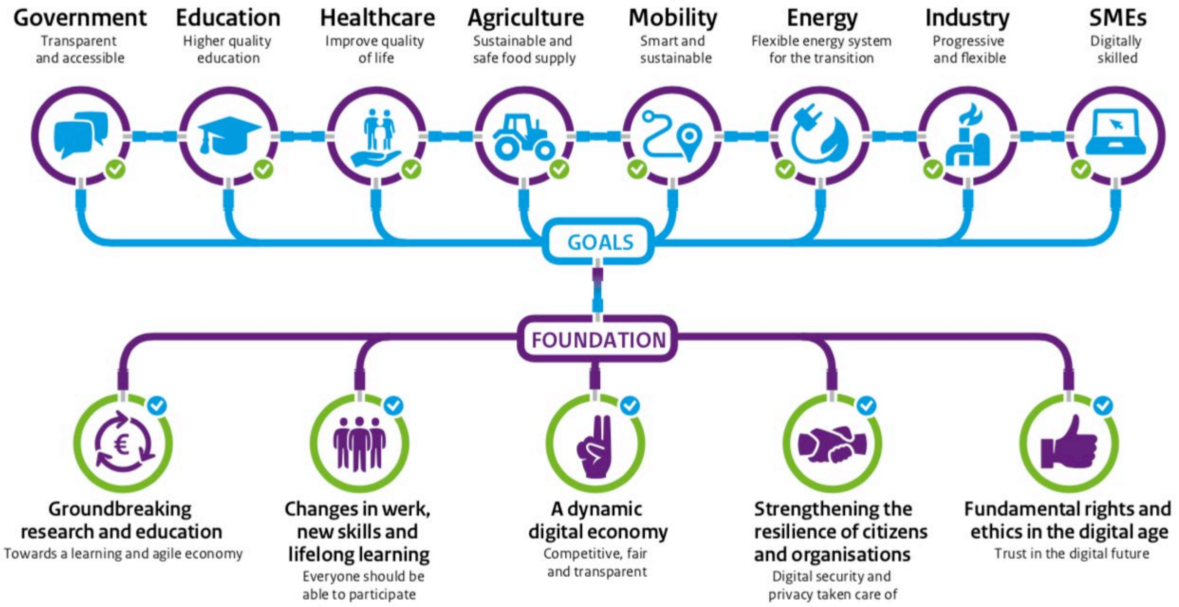
2. Current cybersecurity policy

2.1 Overview of key policy documents

2.1.1 Dutch Digitalisation Strategy

In June 2018 the Ministry of Economic Affairs & Climate published a comprehensive Dutch Digitalisation Strategy (NDS) to give further substance to the challenges and opportunities offered by digitalization. This is the first time that government-wide ambitions and objectives have been formulated for a successful digital transition in the Netherlands. The Dutch government aimed to become the digital leader in Europe and has fully committed to the opportunities offered by the new economy and information society. To achieve this strategy, the Netherlands focusses on eight sectors and five key focus areas.

Diagram NL3: Dutch Digitalization Strategy: sectors and focus areas


Government
Transparent and accessible
Education
Higher quality education
Healthcare
Improve quality of life
Agriculture
Sustainable and safe food supply
Mobility
Smart and sustainable
Energy
Flexible energy system for the transition
Industry
Progressive and flexible
SMEs
Digitally skilled
GOALS
FOUNDATION
Groundbreaking research and education
Towards a learning and agile economy
Changes in werk, new skills and lifelong learning
Everyone should be able to participate
A dynamic digital economy
Competitive, fair and transparent
Strengthening the resilience of citizens and organisations
Digital security and privacy taken care of
Fundamental rights and ethics in the digital age
Trust in the digital future

The digitalization strategy sets the following three ambitions for the identified sectors based through the key focus areas:

1. ***Leading the way and taking advantage of opportunities.*** The Netherlands aims to be a pioneer and testing ground in the field of digital innovation, becoming a place where companies from all over the world can responsibly develop and test new applications, and the place where successful innovations are subsequently rolled out across the country. This will also strengthen Dutch earning capacity and enables the Netherlands to give better direction to technological developments.

2. ***Everyone can participate and work together.*** This goal requires the learning of basic skills and their continued learning in order to adapt to changing occupations. There is also a strong focus on supporting vulnerable groups.

3. ***Trust in the digital future.*** The Dutch government aims to make the upmost efforts to uphold values and fundamental rights such as safety, privacy, self-determination, fair competition, and accessible and good public administration in the digital age. The Dutch Digitalization Strategy states that trust is the foundation of the digital transformation, stating that citizens need to be able to trust that data is secure and that digital technology is used with care. As far as the Dutch Government is concerned, these are the proverbial safety barriers for the digital transformation.

Digitalization of the economy and society requires a digital strategy that is constantly evolving. During the conference Nederland Digitaal, additional inputs were gathered by the Ministry of Economic Affairs and Climate and will result in the release of the second edition of the Dutch Digitalisation Strategy 2 (NDS 2).

2.1.2 National Risk Profile 2016

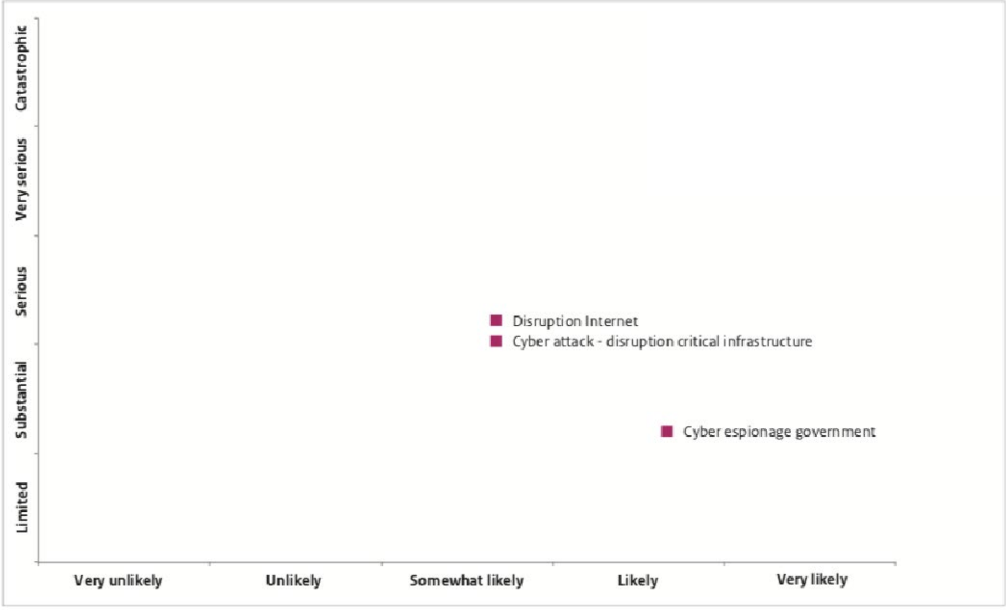
The National Risk Profile (NRP) provides an overview of the risks of various disasters, crises and threats with a possible destabilizing effect on the Dutch society. The NRP is part of the National Safety and Security Strategy which the government uses to investigate which disasters, crises or threats can jeopardize Dutch national security and what can be done about them. The NRP also describes the capabilities which are available to manage the risks and identifies the link and mutual effect between various risks. As a consequence, the NRP constitutes a basis for the next step, which is the capability analysis. The capability analysis involves an investigation to establish which capabilities may have to be strengthened or developed and what kind of measures are required. The NRP uses an all-hazard risk approach to identify a range of threats to Dutch National Security and includes a dedicated section on cyberthreats.

The National Risk Profile combines the annual reports of the Military Intelligence Agency (MIVD) and the annual National Cyber Security Assessments and other research reports that have been made available to the NCTV. The 2016 NRP identifies three main cyberthreats for Dutch National Security:

1. Disruption of the internet;
2. A cyberattack with the goal to disrupt national critical infrastructure;
3. Cyberespionage by government.

The next diagram shows the assessed likelihood and impact for each of these three cyberthreats.

Diagram NL4. Cyberthreats according to National Risk Profile 2016



2.1.3 National Cyber Security Agenda (NCSA)

The National Cyber Security Agenda (NCSA) released in 2018 sets out the framework for the next action items required in cybersecurity. This strategy document lays out a joint governmental direction and considers various measures collectively. This effort has the aim to enhance the impact of public and private actions. The NCSA comprises of seven ambitions that contribute towards the objective of the Netherlands becoming capable of capitalizing on the economic and social opportunities of digitalization in a secure way and of protecting national security in the digital domain. These seven ambitions are the following:

1. The Netherlands aims to develop adequate digital capabilities to detect, mitigate and respond decisively to cyberthreats;
1. The Netherlands aims to contribute to international peace and security in the digital domain;
2. The Netherlands aims to be at the forefront of digitally secure hardware and software;
3. The Netherlands aims to have resilient digital processes and a robust infrastructure;
4. The Netherlands aims to have successful barriers against cybercrime;
5. The Netherlands aims to lead the way in the field of cybersecurity knowledge development;

6. The Netherlands aims to have an integrated and strong public- private approach to cybersecurity

These seven ambitions have been elaborated into objectives and measures that will be implemented in close public-private cooperation. To ensure this, a National Cyber Security Alliance will be formed between government bodies and businesses in which they will commit to jointly strengthening the Dutch approach to cybersecurity.

2.1.4 National Cyber Security Strategy 2 (NCSS 2)

Though the National Cyber Security Agenda is considered by some as the Third National Cyber Security Strategy, the NCSA explicitly states it build upon the National Cyber Security Strategy 2 of 2013 and continues to state in (the Dutch Version[127] of) the NCSA the following vision:

> *Working with international partners, the Netherlands aims to create a secure and open digital domain, in which the opportunities for our society offered by digitisation are used to the full, threats are countered effectively and fundamental rights and values are protected.*[128]

In 2011, the Dutch Government published the first National Cyber Security Strategy. Since then the NCSC-NL has succeeded in gaining better insight into cyberthreats. The Cyber Security Assessments Netherlands has made a more focused approach possible, and furthered the importance of international implementation. Agreements about cooperation, standards of conduct and standards will have to be made in a European, and wider international, context. The international policy context has also become wider. Cybersecurity cannot be achieved in isolation and will have to be approached in correlation with subjects like fundamental rights, values and social-economic benefits. All these developments require taking the next step to achieve a collaborative approach to cybersecurity.

The next table provides a rough idea of the step taken with the NCSS 2 compared to the previous Nations Cyber Security Strategy.

Table NL1. Comparison of NCSS 1 and NCSS 2

National Cyber Security Strategy 1 (2011)	National Cyber Security Strategy 2 (2013)
Public-private partnership	Private-public participation
Focus on structures	Focus on networks / strategic coalitions
Formulation of multi-stakeholder model	Clarifying the relationships between the various stakeholders
Capacity building in the Netherlands	Capacity building both in the Netherlands and abroad
Formulation of fundamental principles	Presentation of (policy) vision
From ignorance to awareness	From awareness to capability

2.1.5 *International Cyber Strategy*

In 2017 the Dutch government presented its International Cyber Strategy – Building Bridges – Towards an integrated international cyber policy. The International Cyber Strategy is complementary to and in line with the National Cybersecurity Strategy (NCSS 2) and the Defence Cyber Strategy. The strategy first explores the international interests, threats and challenges at play in this area and presents the vision and principles underlying the Strategy.

The Dutch government takes an integrated approach to international cooperation on cyber policy. This extends to a variety of areas, such as international cooperation, diplomacy and strengthening international legal frameworks. It also looks at cyberdefense, cybersecurity and capacity building.

In its last chapter, the Dutch Government fleshes out its vision into the following policy priorities:

- Economic growth and sustainable development of the internet;
- Effective internet governance;
- Further enhancement of cybersecurity;
- Effective efforts to stop cybercrime;
- International peace, security and stability;
- Fundamental Rights and online freedom.

[127] The English version of the NCSS2 uses "digital" instead of "cyber"

[128] Dutch National Cyber Security Strategy 2, p7.

2.1.6 National Cyber Security Research Agenda (NCSRA)

The first NCSRA was published in 2009 through the coordination of ICT Innovation Platform Security and Privacy (IIP-VV), and organization now known as dcypher. The first NCSRA recognized the high reliance of Dutch society on digital infrastructures and Stuxnet attack on the Natanz plant highlighted how attackers may target national strategic interests. The first agenda addressed three main core points: to provide confidence and trust in the digital landscape, to provide expertise on strategic digital issues, and to stimulate cybersecurity products and services in the Netherlands. The main focus of the first NCSRA was security and trust and the security and trustworthiness of infrastructure. The second NCSRA focused on offensive capabilities, and aimed to coordinate the research initiatives of the Dutch Top Sector, and to better align with European research. The third and most recent NCSRA took an approach that focused on research directions rather than on research topics in order to stimulate interdisciplinary research. The five research pillars are Design, Defense, Attacks, Governance and Privacy.

2.1.7 Cyber Defense Security Strategy 2018

The 2nd Cyber Defense Security Strategy (2018) was drawn up within the framework of the Defense Memorandum 2018, the Integrated Foreign and Security Strategy (GBVS) and the Dutch Cyber Security Agenda (NCSA) and contributes to the implementation of these strategies. The Defense Memorandum 2018 describes the strategic roadmap for the Dutch Ministry of Defence as a whole. The Integrated Foreign and Security Strategy (GBVS) describes the international approach to the security of the Dutch citizens, the Netherlands and the Kingdom of The Netherlands. The strategy focuses on three pillars: prevention, defense and reinforcement. The Defense Cyber Security Strategy builds on the foundation laid after the publication of the first Defense Cyber Strategy in 2012 with the establishment of the Defense Cyber Command (DCC) and the Joint Sigint Cyber Unit (JSCU) of the AIVD and the MIVD and the strengthening of the Defense Computer Emergency Response Team (DefCERT) and the Royal Netherlands Marechaussee

2.1.8 Other Policy Documents

In addition to the document described before, the Dutch Government has released many more documents derived from that. Examples are the Digital Government Agenda (2019), the Digital Agenda for Primary and Secundary Education, an update Digital Agenda (2018) and the Roadmap Digital Safe Hardware and Software (2018) published by the Ministry of Economic Affairs & Climate as a direct result from the third ambition as defined in the Digitalisation Strategy.

2.2 National cybersecurity strategy: fields, tasks, priorities

The NCSS 2 states that the Dutch Government aims to realize the following ambitions:

- The Netherlands aims to become a leader in cybersecurity:
- For Dutch society to know how to make safe, optimal use of the advantages of digitization.
- Aims for Dutch businesses and the research community to become pioneers in 'security by design' and 'privacy by design'.
- Aims to form a progressive coalition that seeks to protect fundamental rights and values in the digital domain together with its international partners.

Five objective have been defined in the NCSC2 to achieve these ambitions:

- The Netherlands aims to become resilient to cyberattacks and protect its vital interests in the digital domain;
- The Netherlands aims to tackles cybercrime;
- The Netherlands aims to invests in secure ICT products and services that protect privacy;
- The Netherlands aims to build coalitions for freedom, security and peace in the digital domain;
- The Netherlands aims to have sufficient cybersecurity knowledge and skills, and invests in ICT innovation to attain cybersecurity objectives.

The goals of NCSC2 have been outlined in an action program between 2014 and 2016 consisting of 37 actions that are annually reported by Cabinet to the Lower House (Tweede Kamer) of the Dutch Government.

The following themes are part of the action program of NCS2:

1. Risk analyses, security requirements and information sharing within critical infrastructure sectors.
2. More active approach to cyberespionage.
3. Feasibility study on separate vital network.
4. Enhancing civil-military cooperation.
5. Strengthening the National Cyber Security Centre;
6. International approach to cybercrime: updating and strengthening legislation, including the Criminal Code.
7. Supported standards, "security by design" and "privacy by design."
8. Cyber diplomacy: hub for expertise for conflict prevention.
9. Task-force on cybersecurity education.
10. Encouraging innovation in cybersecurity.

2.3 National cyberdefense strategy: fields, tasks, priorities

In July 2012 the Dutch Ministry of Defence published its formal Defence Cyber Strategy outlining the tasks and responsibilities of the armed forces in the newly emerging cyber domain. Before the publication of its own strategy document the Ministry of Defence's contribution to cybersecurity was covered in the first National Cyber Security Strategy, published in 2011 under the responsibility of the Ministry of Justice and Security. The Ministry of Defence's ambitions in the cyber domain may be described as relatively modest compared to the strategies laid out by larger NATO partners such as the USA and the UK, and other larger nations outside the alliance. The Netherlands being a smaller nation with a smaller budget is part of the explanation, but other considerations also play a role. The new digital capabilities of the armed forces will be embedded in an emerging network of various government agencies working within the broader field of cybersecurity and internet governance. Another limiting factor is the fact that most of the infrastructures and computer systems that are vulnerable to cyberattacks are privately owned, privately operated, or belong to public agencies outside of the scope of the military.

In 2015 the Ministry of Defence provided an update of its first Cyber Defence Strategy which was followed by the release of its latest Cyber Defence Strategy in 2018. On the basis of this strategy, the MoD invests in cyber capabilities in order to:

- Be in charge of its own IT and weapon-systems at all times, and to ensure its digital resilience. This will remain an important point of attention in the coming years.
- Gain insight into threat actors on Dutch national security in the digital domain. The MIVD plays an indispensable role together with the AIVD.
- Have more possibilities to disrupt or deter digital attacks.
- Ensure the safety of the Netherlands and its critical infrastructure and processes together with civil partners in the event of an unexpected military conflict involving the use of digital means of attack.
- Use digital means in a targeted manner to obtain and to keep the preponderance in the context of military operations.

2.4 Context/Analysis: key policy principles

Up until 2010 the Dutch government included the topic of cybersecurity within its National Security Strategy (NCSS). This strategy was released in 2007 and a progress report has been released each year thereafter. In 2011 the Dutch government released a number of policy documents including its first national cybersecurity assessment and its first national cybersecurity strategy. The Ministry of Defense released its first defense cybersecurity strategy in the same year. The NCSS acknowledges that cybersecurity is a driver for the Dutch economy as an enabler for innovation, and it also states the importance of a free and open internet. The parallel release of the first National Cyber Security Research Agenda (NCSRA I) indicates that governmental drive for innovation. The NCSS emphasizes both a public-private partnership as well as the duty of citizens, companies, critical infrastructure and government authorities to work together on cybersecurity issues. The NCSS also marked the transition of the Dutch Governmental CERT, previously known as "GovCERT", from its founding in 2002 within the Ministry of Interior, towards the Ministry of Justice and Security as of August 2011. The core task of the NCSC-NL was to create awareness in the Netherlands of the threat landscape, reason for which they have been releasing the Cyber Security Assessments Netherlands every year since.

The second shift in policy aimed to achieve a higher level of maturity for the Dutch cybersecurity landscape. Continuing from the first NCSS the emphasis remained on public-private cooperation and innovation. Again the release of the second National Cyber Security Strategy (NCSS 2) was combined with the release of the second National Cyber Security Research Agenda (NCSRA II). The NCSS 2 calls for the participation of civil society and private industry to achieve a higher level or resilience through cyber hygiene of citizens and responsible behaviors from industry, including suppliers of IT hardware, software and services. Various Ministries facilitate the sharing of threat intelligence and incident information, as well as providing frameworks for national policy, international cooperation and by increasing the capabilities of the NCSC-NL, National Police's High-Tech Crime Unit (HTCU) and both the military and civilian intelligence agencies, the MIVD and AIVD respectively. The goals of NCSC2 has been outlined in an action program between 2014 – 2016 consisting of 37 actions that are annually reported to the Lower House (Tweede Kamer) of the Dutch Government.

In 2018 these 37 actions were updated in the National Cyber Security Agenda (NCSA). The NCSA states that is not a replacement of NCSS 2, but builds further upon the effects that were realized with previous the National Cyber Security Strategies from 2011 and 2013.

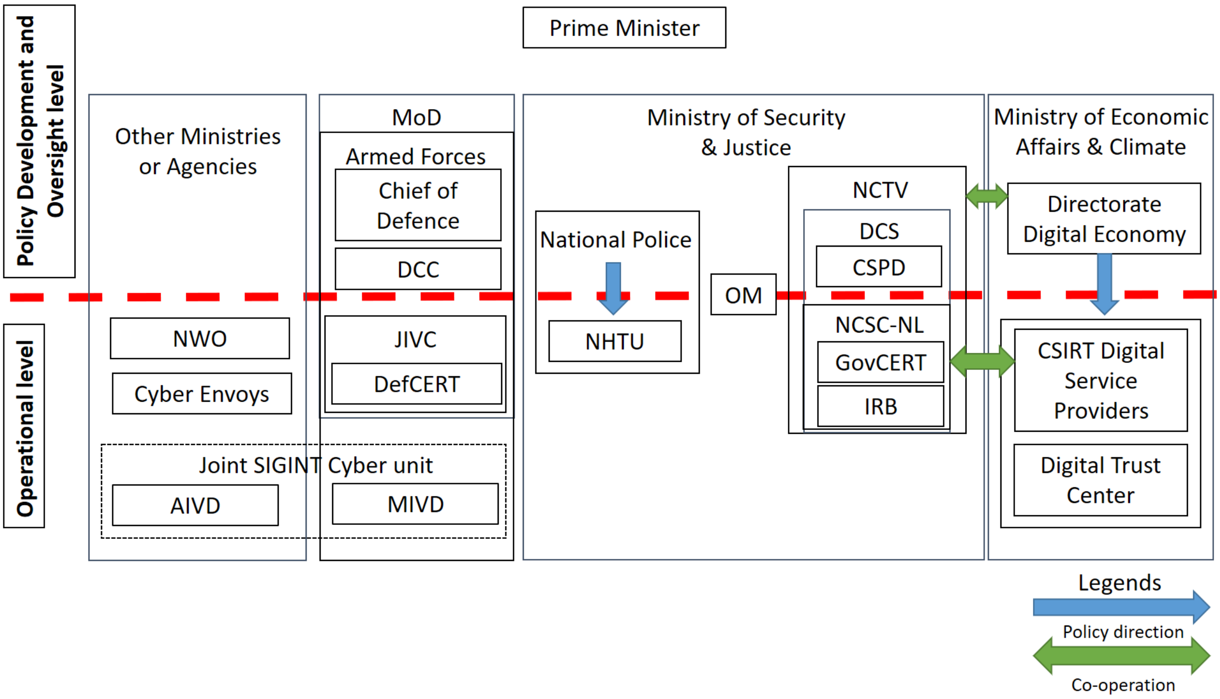
The policy shift in The Netherlands that took place since 2017 and 2018 is much larger than originally perceived. Until 2018, issues such as privacy and digital security in particular were on the policy agendas of various ministries. Little attention was paid to an overarching vision of the significance of digitization. This changed with the release of a single joint strategy in the area of digitalization, impacting almost all policy areas. The government wants the Netherlands to lead the way in the application of new technology. To achieve this, the Dutch government is strengthening the foundation for digitalization, in the field of privacy, cybersecurity, digital skills and fair competition, among other things. The National Cyber Security Agenda, and again the third National Cyber Security Research Agenda (NCSRA III) and the new cyberdefense strategy by the Ministry of Defence now all have an overarching strategy to achieve that ambition. Finding the right balance between the many organizations involved, and primarily between using the opportunities digital technology and cybersecurity in both policies as well as responsibilities will become the Dutch challenge in the forthcoming years.

3. Current public cybersecurity structures and initiatives

3.1 Overview of national organization framework

Of the many different ministries and government organizations with individual and collective responsibilities for enhancing the cybersecurity posture of the Netherlands, the diagram below shows those organizations where the majority of the operational activities can be found.

Diagram NL5: Oversight Organigram



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

3.2.1 Dutch National Cyber Security Center (NCSC-NL)

The **National Cyber Security Center** (NCSC-NL) of the Ministry of Justice & Security operates under the commissioning of the National Coordinator for Security and Counterterrorism (NCTV) executed by The Cyber Security Directorate. The Director of Cyber Security Directorate is also the deputy National Coordinator for Security and Counterterrorism. NCSC-NL responds to cyberthreats and incidents and works to strengthen a safe and resilient digital society. The NCSC-NL is a key-player in enhancing the resilience of the Netherlands in the digital domain. The goal of the NCSC-NL is to realize a safe, open and stable information society by sharing knowledge, providing insight and pragmatic advice. The primary target group of NCSC-NL is the Dutch central government and operators in the critical infrastructure. The NCSC-NL

For its primary target group, the NCSC-NL acts as the national CERT. Within the remits and legal boundaries of NCSC-NL, defined by the 2018 adapted new law “Wet Beveiliging Netwerk- & Information Systemen” (law for secure networks and information systems), the main activities of NCSC-NL were defined as:

a. Assisting operators of central government and vital infrastructures in taking measures to safeguard or restore the availability and reliability of their products or services;
b. Informing and advising these operators and others in and outside the Netherlands on threats and incidents with respect to the information systems referred to in the opening words;
c. Conducting analyses and technical research for the benefit of the duties set out under a and b, following the threats and incidents referred to under b or indications thereof.

Since the publication of the Dutch first National Cyber Security Strategy, the NCSC-NL has absorbed the former GovCERT and plays a crucial role in crisis management, in the case of IT-related crises, and stimulates public-private partnerships, as well as other collaboration efforts with regards to information sharing.

3.2.2 Digital Trust Center

The **Digital Trust Center** (DTC) is a 3-year program from the Ministry of Economic Affairs & Climate that aims to help entrepreneurs in securing their digital businesses. The target group of the DTC consists of 1.6 million companies including freelancers, medium enterprises, and large companies. These are all companies in the Netherlands that do not belong to the critical industry, such as banking, telecom, energy and water companies. Companies in these critical sectors have the National Cyber Security Center (NCSC-NL) as cooperation partners within the national government.

The DTC supports the companies through a digital platform with up-to-date information and reliable advice, and a yearly subsidy scheme for companies in their target group that are looking for cooperation. The DTC works closely with the NCSC-NL to make relevant current threat information collected by the NCSC-NL for national government and critical infrastructure accessible to entrepreneurs. The DTC also works closely with a growing group of network partners such as sector organizations, semi-public institutions, regional company cluster organizations, knowledge institutes and market parties. Collectively, the DTC aims to look for new ways to enable entrepreneurs to be safer in digital business.

3.2.3 CSIRT Digital Service Providers

The European Directive for Network and Information Security Directive (NIS Directive) led to the establishment of the **CSIRT Digital Service Providers** (CSIRT DSP) under the Ministry of Economic Affairs & Climate since the Netherlands consider Digital Service Providers non-CNI. The task of the CSIRT DSP is to receive reports of incidents from digital service providers with the aim of limiting the economic and possibly social damage of an incident. The CSIRT DSP may also warn other digital service providers if a certain type of incident occurs and shares current threat information.

The CSIRT DSP works closely with the NCSC-NL in the execution of its activities, the sharing of information and the (inter)national collaboration where the NCSC-NL is the designated national point-of-contact. The CSIRT DSP is currently a program along the evaluation timeline of the DTC4.

3.2.4 Cyber Security Council (CSR)

The second National Cyber Security Strategy (NCSS 2) also called for the creation of a **Dutch Cyber Security Council** (Cyber Security Raad, CSR) to serve as a national and strategic advisory body. The CSR became operational in June 2011 and was tasked with providing strategic guidance to the Dutch Cabinet on cybersecurity matters and advises on the implementation and development of the national cybersecurity strategy, contributes to the Dutch Cyber Security Research Agenda (NCRSA) by highlighting future requirements for national research and development and promotes cybersecurity awareness among senior leaders in the private sector through a series of board room dialogues. The CSR is a unique private-public partnership comprised of 18 members, seven from government, seven from private industry, and four from the scientific community.

The Cyber Security Council (CSR) is a national and independent advisory body to the government and is composed of high-level representatives from public and private organizations and knowledge institutes. The CSR operates on a strategic level to increase the level of cybersecurity in the Netherlands. The CSR's unique multi-stakeholder composition aims to make it possible to strategically approach priorities, bottlenecks and incidents from various angles and to develop an integrated vision of opportunities and threats. The CSR seeks cooperation with similar councils in other countries and encourages their creation in countries that do not yet have a Cyber Security Council. The CSR has the following tasks:

- Solicited and unsolicited provision of advice to the government and private parties.
- Advise on the implementation of the national cybersecurity strategy.
- Providing a contribution to the National Cyber Security Research Agenda.
- Advising the crisis organization in the Netherlands during large-scale cyber-incidents.

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

The MoD perceives that properly established defense and security are not enough to prevent threat actors from performing digital attacks. The Netherland is joining a wider trend known as "active defense" as other nations also begin to take a more active stance in digital defense. In the context of both the first and third core tasks of the MoD, a more active defense contribution is necessary within existing structures. To reinforce this, the MoD aims to invest in six capabilities and concepts during the coming years:

1. Information: capacity to act and attribution.
2. Contribute to deterrence through its military assets in the digital domain.
3. Digital resilience and protection of own networks and systems.
4. Research into national fallback options.
5. Military assistance and support to civilian authorities.
6. Law enforcement (Royal Netherlands Marechaussee).

Article 97 of the Constitution for the of the Netherlands states that a Dutch armed force exists, including for “the purpose of maintaining and promoting the international legal order.” The reference in this article to the international legal order is closely linked to Article 90, which states that the government will promote international rule of law. This means the Netherlands is committed to promoting the international legal order, conflict prevention and stabilization. Due current geopolitical trends on the boarder countries to the European Union, this second core task may require a lot more effort from the MoD in the coming years. The Netherlands also contributes to this by taking an integrated approach to military missions and operations in an alliance.

The cyberdefense strategy outlines the developments and priorities that should lead to the MoD being able to effectively implement its three main tasks in the digital domain. Though this is their ambition, the following are prerequisites that will require further strategic attention of the MoD: personnel, knowledge development and innovation, and cryptography. In addition to the Military Intelligence & Security Department two main units are involved in cyber-operations within the Dutch MoD:

3.3.1 DefCERT

The Defense Computer Emergency Response Team (DefCERT) is deployed to ensure that military operations are not hampered and the Defense information systems are reliable. For this, DefCERT must:

1. see cyberthreats on time;
2. investigate how great the threat is;
3. ensure that the threat diminishes or disappears

In addition, DefCERT can also support civil authorities in coordinating cyberthreats. DefCERT works closely with other teams when performing its duties, such as NCSC-NL, the NATO Computer Incident Response Capability (NCIRC) and within the Forum of Incident Response and Security Teams (FIRST).

3.3.2 Defense Cyber Command

Defense Cyber Command. This organization falls directly under the Commandant of the Armed Forces. The cyber command is committed to the digital security of the entire Defense organization and its partners. The Defense Cyber Command focuses on three areas of digital security:

1. *Defense*. All digital systems must be safe from attacks and espionage;
2. *Information*. The armed forces must be aware of threats in the digital environment. These threats come both from within one's own systems (weaknesses and "back doors") and from outside. The cyber command must be able to infiltrate into third-party systems to obtain information about cyberthreats;
3. *Attack*. The armed forces can attack, manipulate or switch off digital systems of opponents. Opponents can be other countries, but also (terrorist) organizations or hackers.

3.3.3 Cyber-Reserve

The Dutch MoD also successfully set-up a **cyber reservist** program. Cyber reservists are civilian cybersecurity specialists in the technical and functional domains from The Netherlands, which the MoD may call upon in case of cyber calamities and for military operations. Cyber reservists not only have sufficient technical knowledge, but also the necessary creativity and skills to use this technical knowledge effectively. The shortage of cyber professionals also appears to be structural, given the low numbers of students graduating with IT specialization every year at Applied Sciences and University levels (HBO and WO). These numbers are currently insufficient to meet the regular demand from IT employers. The MoD has therefore also stated in their Cyber Defense Strategy that they consider the use of cyber reservists as a solution for dealing with the identified shortage of specialists. The possibility of becoming a cyber reservist attracts people who are already working in the cybersecurity domain and are, or would like to be, familiar with the defense organization as reservists. The MoD aims for reservists to get started quickly and efficiently when necessary. It is a way to deal more efficiently with scarce expertise. The DigiNotar incident shows that a sudden need for upscaling and a shift in capacity actually occurs in practice. The Defense organization made its contribution in settling this incident by making capacity available from the DefCERT team.

3.4 Context: key public organizational framework

Continuous, consistent and sufficient information by national cyber risk assessments and national security profiles provides the risk perception necessary to ensure successful outcomes to an ambitious agenda. Not having a central authority to manage and track the milestones against clearly defined timeframes may reduce the effectiveness of an overall strategy in the Netherlands. The Dutch approach to managing national cyber risk is still typically decentralized and depends on the "polder" model of cooperation. There are at least 20 different ministries and government organizations with individual and collective responsibilities for enhancing the cybersecurity posture of the Netherlands, but no single agency has overarching authority to ensure the national cybersecurity architecture is achieved. This requires an additional effort to find appropriate alignment between the many strategies developed by the involved ministries and government organizations. Achieving the ambition to become a leader in cybersecurity, as defined by the Cabinet, requires the alignment of the national digitalization strategy, the national cybersecurity agenda, the national cyberdefense strategy and the national cybersecurity research agenda. This concerns a complex challenge that requires appropriate analysis to identify the key differences and ensure alignment in execution. Deciding on effective approach through a risk-based approach requires the identification of the 'risk-appetite' of all involved organizations through a shared framework such as a social contract for cybersecurity.

The polder model is based on Dutch social traditions and socio-cultural backgrounds and is rooted in social traditions and cultural backgrounds. The post WWII Netherlands was built through consensus formation and common commitment, although at that time the hierarchy and top-down structures were still paramount. In the 1980s, joint effort and responsibility were given shape and content in a new way through the polder model of consensus. The policy choices made by the current government coalition are characterized by a model in which government control is sometimes the dominant factor, while at other times it's market forces.

Cybersecurity required high trust economies as described by Francis Fukuyama and Alain Peyrefitte. Trust involves more than being able to count on each other. It also has to do with bearing social responsibility, with having a vision of a good society and with attention to moral foundations. The polder model is not only successful because good and trustworthy agreements are being made. It acquires meaning because it is supported by a 'culture of responsibility' that is well applicable in the field of cybersecurity with it every increasing connected ecosystem.

However, effective implementation of the national strategies requires leadership and governance that defines and clarifies roles, responsibilities, processes, governance, and accountability. The NCSA is committed to an integrated cybersecurity approach. This requires a joint effort from the business community, social organizations and various government parties. In 2018, various policy documents from various ministries provided guidance on cybersecurity. Attention has been given to mutual coordination between many ministries and government organizations involved in the development of these strategies. This process is still ongoing and requires attention during the execution of the various plans through the underlying polder model and the actions that were defined.

The various ministries and government organizations must make a coherent case to increase efforts by both government, private parties, civil society as well as science. The government plays a strong role in this and looks at positive incentives to shape the required cooperation. Figures from various scientific researchers show that the number of investments in cybersecurity research has continued to fall in recent years. Investing in scientific knowledge is now important in view of the fact that the increasing demand and the imminent shortage of cybersecurity professionals are a global issue and more cybersecurity professionals are moving abroad in the Netherlands and potentially causing a brain-drain.

Initiatives from the European Union have also affected the Dutch landscape. This was the case with initiatives that require coordination, such as the Network and Information Systems Security Act (Wet beveiliging netwerk-en informatiesystemen, Wbni), which was a result from the Network and Information Security Directive (NIS Directive) which led to the establishment of the CSIRT DSP, and the proposal for the new European cybersecurity regulation of the European Union. The coordination of both the content and the implementation of the various strategies, legal frameworks and agendas is a precondition for the development of an integrated approach.

4. Cyberdefense and Cybersecurity partnership structures and initiatives

4.1 Public-Private cyberdefense partnerships

In the national context, NCSC-NL cooperates with other government agencies, as well as with private organizations. Examples of these partners include the National Police, General Intelligence and Security Service (AIVD), Military Intelligence and Security Service (MIVD), Dutch Telecom Authority (ACM), Radiocommunications Agency Netherlands (AT), National Forensic Institute (NFI), Public Prosecutor office (OM), Dutch internet service providers, other incident response teams in The Netherlands, organizations in critical infrastructure, and several other organizations. The NCSC-NL participates in Information Sharing and Analysis Centers (ISAC's) with organizations in the critical infrastructure sector.

In addition to that, the NCSA has structured many of the public-private partnerships on cyberdefense in the Cyber Security Alliance (CSA). In the CSA, public and private organizations aim to work together on complex and diverse issues by realizing breakthroughs in concrete projects. As of May 2018, several public and private parties have signed a letter of intent to cooperate. The Alliance is an independent, inclusive network and platform for public-private cooperation in the field of cybersecurity. The alliance's independence means that the execution of projects is not linked to a particular stakeholder, and decisions on projects are also not bound to one particular stakeholder. The Cyber Security Alliance has an open invitation for organizations in the Netherlands to register a project and become part of the initiative which currently includes three projects. In addition to the Cyber Security Alliance projects, many other things are taking place that help to make the Netherlands digital resilient. The Cyber Security Alliance offers an overview of all current cyber initiatives, ranked according to the objectives of the NCSA.

4.2 International cyberdefense partnerships

The NCSC-NL is part of an extensive network of affiliated organizations. These sorts of organizations are referred to as Computer Emergency Response Teams (CERTs). Since this network is a vital information hub, the NCSC-NL finds it important to make expertise available to other teams for the benefit of the international CERT community. Given the previous description of the Netherland's financial limitations, the aim is to achieve maximum results with minimum means, and international collaboration is one way to realize this. Due to this, the NCSC-NL encourages the development of shared standards and specialization in different areas. Their primary network is the Computer Security Incident Response Team (CSIRT) network under the NIS Directive that establishes in article 12 a CSIRTs network "in order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational."

Cyberdefense has also been integrated into NATO's Smart Defence initiatives in which the Netherlands is an active participant. Smart Defence enables countries to work together to develop and maintain capabilities they could not afford to develop or procure alone. This also allows countries to free resources for developing other capabilities. The Smart Defence projects in cyberdefense thus far include the Malware Information Sharing Platform (MISP), the Smart Defence Multinational Cyber Defence Capability Development (MN CD2) project, and the Multinational Cyber Defence Education and Training (MN CD E&T) project.

The Netherlands is also an active member of the Cooperative Cyber Defence Centre of Excellence that was established on 14 May 2008 and was fully accredited by NATO on 28 October 2008. NATO Cooperative Cyber Defence Centre of Excellence is an International Military Organisation with a mission to enhance the capability, cooperation and information sharing among NATO, its member nations and partners in cyberdefense by virtue of education, research and development, lessons learned and consultation. Between 2009 and 2012 a Dutch representative of the Ministry of Defence led an international group of approximately 20 experts to develop the Tallinn Manual (originally entitled, Tallinn Manual on the International Law Applicable to Cyber Warfare) in 2013 and the update to Tallinn Manual 2.0 in 2017.

4.3 Cyberdefense awareness programs

Alert Online is an initiative that facilitates government, business, education, science and consumers in the Netherlands and to work together on cybersecurity and make them to have more secure data in cyberspace. Alert Online intends to initiate a movement and make consumers more aware of their online activity and digital security, and to strengthen their digital resilience. During the year, Alert Online organizes various activities, in cooperation with other partners, to draw attention to cybersecurity. The most prominent month for this initiative is the month of October, as it is also the European Cyber Security Month. The Alert Online awareness campaign is co-financed by the European Union's Internal Security Fund.

Alert Online started in 2012 on the initiative of the National Coordinator for Counterterrorism and Security. Since 2013 there has been a theme every year, namely: "Smart Security" (2013), "Knowledge" (2014), "Digital Corporate Social

Responsibility" (2015), "Cyber Skills" (2016) and in 2017 and 2018 "Cyber security Heroes ". In 2016 and 2017 Alert Online was organized with more than 200 partners.

4.4 Cyberdefense education and training programs

NATO held the International Crisis Management Exercise (CMX) in 2016 and 2017. This exercise is combined with the international NATO exercise 'Cyber Coalition 12'. With these exercises the participants get insight into the crisis management procedures and cyberdefense capabilities are tested. A scenario was used with an escalating threat of chemical, biological and radioactive attacks and there were also major cyberattacks on the critical infrastructure of different nations and NATO.

The National Cyber Security Center (NCSC) aims to also participate in Cyber Coalition in 2019 as a counterpart for various defense organizations in the Netherlands. To this end, the NCSC-NLhas in particular cooperated with Taskforce Cyber and DefCERT. Consultations and action were taken at various times during the exercise. The exercise Cyber Coalition 12 underlines the importance of joining forces in times of crisis.[129]

4.5 Cyberdefense research programs

The Dutch government cooperates with the NATO CCDCOE for its extensive cyberdefense research. The Netherlands joined NATO CCDCOE in 2012 as a sponsoring nation bringing the total number of nations actively participating in the work of the CCDCOE to 11. As a sponsoring nation, the Netherlands sends their experts to work in the Centre and also contributes to the shared budget.

The MoD carries out most of its cyberdefense research through the Netherlands Defense Academy. This military academic institution has focused its research on various sub-topics relating to cyber-operations in conflict theater. Dutch academia and research institutes are usually involved but are also work closely with the Ministry of Economic Affairs & Climate and the Ministry of Justice & Security. Each research is closely related to the policy domains of each Ministry and cooperation therefore occurs often. An example of this is the holistic approach taken to securing Critical National Infrastructure in The Netherlands through the development of a multi-sector testbed. In addition to addressing the security concerns within CNI, this approach could positively influence the economic performance and position of the Netherlands.

The NCSRAIII has two themes dedicated to cyberdefense research. The “defense” theme focuses on research to increase effectiveness and efficiency of defensive measures in terms of detecting, understanding and mitigating attacks. The key research points for this theme are automated defense systems, intrusion detection, and attack containment and deception. The “attack” theme focuses on research concerning the attack surface of modern digital ecosystems. The key research points for this theme are automation of vulnerability detection and exploit generation, human factors in cyberattacks, and finding new attack vectors. The MoD has actively contributed to the creation of this agenda. As of 2019, the MoD will expand available means for research in the field of cyber. The MoD will invest almost 6.5 million euros per year in cybersecurity research from 2019 onwards, which is an increase from the 4 million euros in previous years. Where possible, this is done together with other departments, as also announced in the Dutch Digitalization Strategy.

[129] NCSC-NLNews item 16-11-2012, NAVO-oefening 'Cyber Coalition 12'

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 NL6: Spectrum of Centralization vs Decentralization of policy development and management

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

5.2 Civilian vs defense posture and oversight

Diagram NL7: Spectrum of Civilian-Defense cybersecurity posture and oversight

Civilian oversight ---X-- Defense

5.2 Offensive vs defensive capabilities

Diagram NL8: Spectrum of Offensive vs Defensive cyberdefense capabilities

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

6. Annex 2: Key definitions

The following key definition originate from the 2018 Cyber Security Assessment Netherlands glossary:

Term	Definition
Digital attack	A digital attack is an intentional breach of cybersecurity.
Cybercrime	A form of crime aimed at IT or the information processed by an IT system. There are various types of cybercrime: • in the narrow sense, a type of criminal activity which targets IT (high-tech crime); • a type of criminal activity where the use of IT is a prime consideration in its perpetration (cybercrime); • in a broad sense, any form of (traditional) criminal activity where IT is used (digital crime).
Cybersecurity	Cybersecurity is the entirety of measures to prevent damage caused by disruption, outage or misuse of IT and repair it should it occur. This damage could comprise impairing the availability, confidentiality or integrity of information systems and information services and information stored on them.
Espionage	Impairing the confidentiality of information by state or state-sponsored actors copying or removing information.
Hacker/Hacking	The most conventional definition of a hacker (and the one used in this document) is someone who attempts to break into IT systems with malicious intent. Originally, the term hacker was used to denote someone using technology (including software) in unconventional ways, usually with the objective of circumventing limitations or achieving unexpected effects.
Incident	An incident is an event where information, information systems or information services are disrupted, fail or are misused.
Information security	Information security is the process of establishing the required reliability of information systems in terms of confidentiality, availability and integrity, as well as implementing, maintaining and monitoring a coherent set of corresponding security measures.

7. Annex 3: Abbreviations

Term	English	Dutch
AIVD	General Intelligence & Security Department	Algemene Inlichtingen- en Veiligheidsdienst
CSA (Academy)	Cyber Security Academy	Cyber Security Academy
CSA (Alliance)	Cyber Security Alliance	Cyber Security Alliantie
CSBN / CSAN	Cyber Security Assessment Netherlands	Cyber Security Beeld Nederland
CISRT DSP	CSIRT for Digital Service Providers	CSIRT voor Digitale Dienstverleners
CSR	Cyber Security Council	Cyber Secyrity Raad
CMX	Crisis Management Exercise	Crisisoefening
DCC	Defense Cyber Command	Defensie Cyber Commando
DefCERT	Defense Computer Emergency Response Team	DefCERT
DTC	Digital Trust Center	Digital Trust Center
FIRST	Forum of Incident Response and Security Teams	
JSCU	Joint Sigint Cyber Unit	Joint Sigint Cyber Unit
MIVD	Military Intelligence & Security Department	Militaire Inlichtingen- en Veiligheidsdienst
NATO	North Atlantic Treaty Organization	Noord Atlantische Verdrags Organisatie
NCIRC	NATO Computer Incident Response Capability	
NCSC-NL	National Cyber Security Center Netherlands	Nationaal Cyber Security Centrum Nederland
NCSRA	National Cyber Security Research Agenda	Nationale Cyber Security Research Agenda
NCSA	National Cyber Security Agenda	Nationale Cyber Security Agenda
NCSS	National Cyber Security Strategy	Nationale Cyber Security Strategie
NCSS 2	National Cyber Security Strategy 2	Nationale Cyber Security Strategie 2
NCTV	National Center for Terrorism & Safety	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NIS Directive	EU Directive on Network & Information Security	EU NIB-Richtlijn
NRP	National Risk Profile	Nationaal Risico Profiel
WBNi	Network & Information Systems Security Act	Wet Beveiliging Net- en Informatiesystemen

8. Bibliography

Bierens (2016). Cyberstrategie is mensenwerk, CSR Magazine (pp 58-60), The Hague

Bierens, Klievink, van den Berg, J. (2017). A Social Cyber Contract Theory Model for Understanding National Cyber Strategies. Proceedings of International Conference on Electronic Government 2017. (pp. 166-176). (Lecture Notes in Computer Science; Vol. 10428). Springer. DOI: 10.1007/978-3-319-64677-0_14

Broeders (2014). Investigating the Place and Role of the Armed Forces in Dutch Cyber Security Governance, Erasmus University, Rotterdam

Castellon, Frinking (2015), Securing Critical Infrastructures in the Netherlands: Towards a National Testbed, HSD, The Hague

Castellon, Gehem, Wijninga, de Spiegeleire, Bekkers, Ginn Mukena, Miladinova (2015) Special Operation Forces: Shadow warriors in light of the future, HCSS, The Hague

CCDCOE (2012) National Cyber Security Framework Manual. NATO CCD COE Publications.

Hathaway (2018). Ambition vs. Progress: The National Cyber Security Agenda of the Netherlands, CSR Magazine (pp 34-36), The Hague

Hathaway (2017). Netherlands Cyber Readiness at a Glance, Potomac Institute, Washington

Internet Security Alliance (2016). The Cybersecurity Social Contract - Implementing a Market-Based Model for Cybersecurity. Internet Security Alliance, Arlington County, Virginia.

Luiijf (2013). Ten National Cyber Security Strategies - A Comparison, The Hague.

Luiijf (2013). Nineteen national cyber security strategies. International Journal for Critical Infrastructures, 9, 3-31.

Luiijf (2014). Nationale Cyber Security Strategie 2 – Van Bewust naar Bekwaam, Magazine Informatiebeveiliging

Ministry of Defence (2012). Defence Cyber Strategy 1, The Hague

Ministry of Defence (2013). Defence Cyber Strategy 1 - Update 1, The Hague

Ministry of Defence (2015). Defence Cyber Strategy 1 - Update 2, The Hague

Ministry of Defence (2018). Defence Cyber Strategy 2, The Hague

Ministry of Economic Affairs & Climate (2018). Dutch Digitalization Strategy, Directorate Digital Economy, The Hague

Ministry of Economic Affairs & Climate (2018). Roadmap Digitaal Veilige Hard- en Software, Directorate Digital Economy, The Hague

Ministry of Economic Affairs & Climate (2018). Digitale Agenda - Vernieuwen-Vertrouwen-Versnellen, The Hague

Ministry of Economic Affairs & Climate (2019). Opbrengsten Conferentie Nederland Digitaal, The Hague

Ministry of Foreign Affair (2017). International Cyber Strategy – Building Bridges – Towards an integrated international cyber policy

Ministry of Interior (2011). National Cyber Security Strategy 1, The Hague

Ministry of Justice & Security (2011). Stuxnet - een geavanceerde en gerichte aanval, NCTV, The Hague

Ministry of Justice & Security (2011). Rapport Diginotar, NCTV, The Hague

Ministry of Justice & Security (2011). National Security Strategy, NCTB, The Hague

Ministry of Justice & Security (2011). Cyber Security Assessment Netherlands, NCSC, The Haguee

Ministry of Justice & Security (2012). Diginotar Black Tulip Update, NCTV, The Hague

Ministry of Justice & Security (2012). Cyber Security Assessment Netherlands, NCSC, The Hague

Ministry of Justice & Security (2013). National Cyber Security Strategy 2, NCTV, The Hague

Ministry of Justice & Security (2013). Leidraad Nationale Veiligheid, NCTV, The Hague

Ministry of Justice & Security (2013). Cyber Security Assessment Netherlands, NCSC, The Hague

Ministry of Justice & Security (2014). Cyber Security Assessment Netherlands, NCSC, The Hague

Ministry of Justice & Security (2015). Cyber Security Assessment Netherlands, NCSC, The Hague

Ministry of Justice & Security (2016). Cyber Security Assessment Netherlands, NCSC, The Hague

Ministry of Justice & Security (2016). National Risk Profile 2016, NCTV, The Hague

Ministry of Justice & Security (2017). Cyber Security Assessment Netherlands, NCSC, The Hague

Ministry of Justice & Security (2018). Cyber Security Assessment Netherlands, NCSC, The Hague

Ministry of Justice & Security (2018). Nederlandse Cybersecurity Agenda, NCTV, The Hague

Ministry of Justice & Security (2018). Cyber Security Radar Netherlands, NCSC, The Hague

Tilburg Institute for Law, Technology and Society (2015). The Governance of Cybersecurity - A Comparative Quick Scan of Approaches in Canada, Estonia, Germany, Netherlands and the UK, Tilburg University, Tilburg.

Rathenau Instituut (2017). Opwaarderen - Borgen van publieke waarden in de digitale samenleving, The Hague.

Rathenau Instituut (2018). Doelgericht Digitaliseren, The Hague, The Hague

Singapore

Francis Domingo
De La Salle University

Highlights/Summary:

1. Key national trends

Singapore is a small but highly developed state in Southeast Asia. Due to historical antecedent and resources competition with its neighbors, it is actively developing both its hard and soft power. More specifically, it is focused on building a Smart Nation and establishing itself as the most highly networked state in the world. This has, however, come at the cost of making Singapore increasingly vulnerable to cyberattacks, which has translated into making cybersecurity a critical national security issue

2. Key policy principles

2.1 Cybersecurity

The Singaporean approach to cybersecurity has evolved from a purely state focused one towards a both comprehensive and holistic one. Specifically, it focuses on four main pillars: 1) fostering resilience of Critical Information Infrastructures; 2) creating a safe cyberspace through whole of society measures, which include cybercrime prevention and public private partnerships; 3) developing a vibrant cybersecurity architecture through capacity building, education, R&D and supporting start-up ecosystems; 4) pursue international cooperation, notably with ASEAN.

2.2 Cyberdefense

Singapore does not have a dedicated cyberdefense strategy but its initiatives in this area are subsumed within the 2016 Cybersecurity Strategy that is aligned with the state's Total Defense strategy, which requires all sectors of society to develop a robust and proactive capability to respond to national security threats. As such, the core cyberdefense principles are purely defensive in nature with a focus on the protection of its key governmental and military infrastructures and sector by the recently created Defense Cyber Organization (DCO).

3. Key national framework

3.1 Cybersecurity

The organizational structure of the Singaporean cybersecurity is centralized around the Cyber Security Agency (CSA), which is co-managed by the Prime minister's office and the ministry of Communication and information. This agency is responsible for supervising cybersecurity policy, operation, education, outreach, and ecosystem development in Singapore at all level of government.

3.2 Cyberdefense

The Defense Cyber Organization of the Singaporean defense forces leads the efforts in securing networks and systems across the Defense Sector and its Defense Cluster. It is notably in charge of providing situational threat awareness, developing cyberdefense capabilities and ensuring resilience of military infrastructure. As such, it closely cooperates and supports its civilian counterparts, such as the CSA.

4. Level of partnership and resources

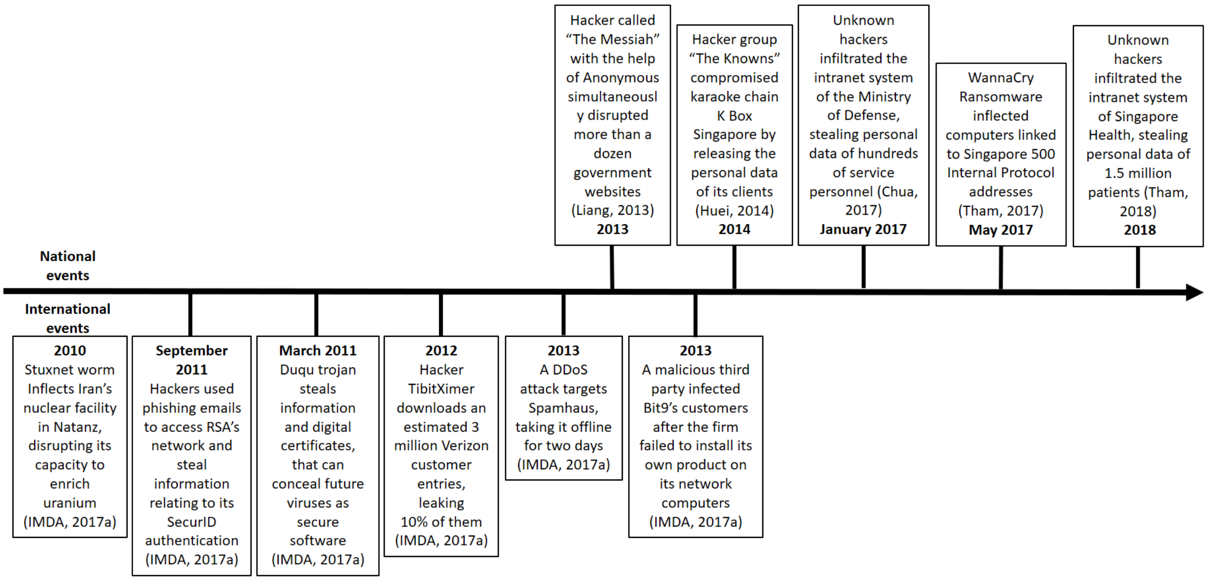
Singapore cybersecurity and cyberdefense partnerships revolve mainly, at regional level, with ASEAN (e.g. crisis response and reporting mechanisms, cybercrime) and, at the international level, with partners such as France and the US with whom it has signed Memorandum of Understandings to strengthen national cyber capabilities. In addition, Singapore also actively promotes private sector partnership, R&D and involvement in cybersecurity through the establishment of dedicated PPPs, such as the Partnership for the Advancement of the Cybersecurity Ecosystem (PACE).

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

1.1 Threat perception: trigger events

This sub-section describes the main domestic and international events that directly or indirectly contributed to the development of Singapore's cybersecurity strategy. Note that the data for these incidents are taken from media articles such as The Straight Times, Today, as well as official documents released by the Infocomm Media Development Authority of Singapore and the Singapore Cyber Security Agency.

Diagram SG1: Timeline of Trigger events



National events

Hacker called "The Messiah" with the help of Anonymous simultaneously disrupted more than a dozen government websites (Liang, 2013) **2013**

Hacker group "The Knowns" compromised karaoke chain K Box Singapore by releasing the personal data of its clients (Huei, 2014) **2014**

Unknown hackers infiltrated the intranet system of the Ministry of Defense, stealing personal data of hundreds of service personnel (Chua, 2017) **January 2017**

WannaCry Ransomware inflected computers linked to Singapore 500 Internal Protocol addresses (Tham, 2017) **May 2017**

Unknown hackers infiltrated the intranet system of Singapore Health, stealing personal data of 1.5 million patients (Tham, 2018) **2018**

International events

2010 Stuxnet worm Inflects Iran's nuclear facility in Natanz, disrupting its capacity to enrich uranium (IMDA, 2017a)

September 2011 Hackers used phishing emails to access RSA's network and steal information relating to its SecurID authentication (IMDA, 2017a)

March 2011 Duqu trojan steals information and digital certificates, that can conceal future viruses as secure software (IMDA, 2017a)

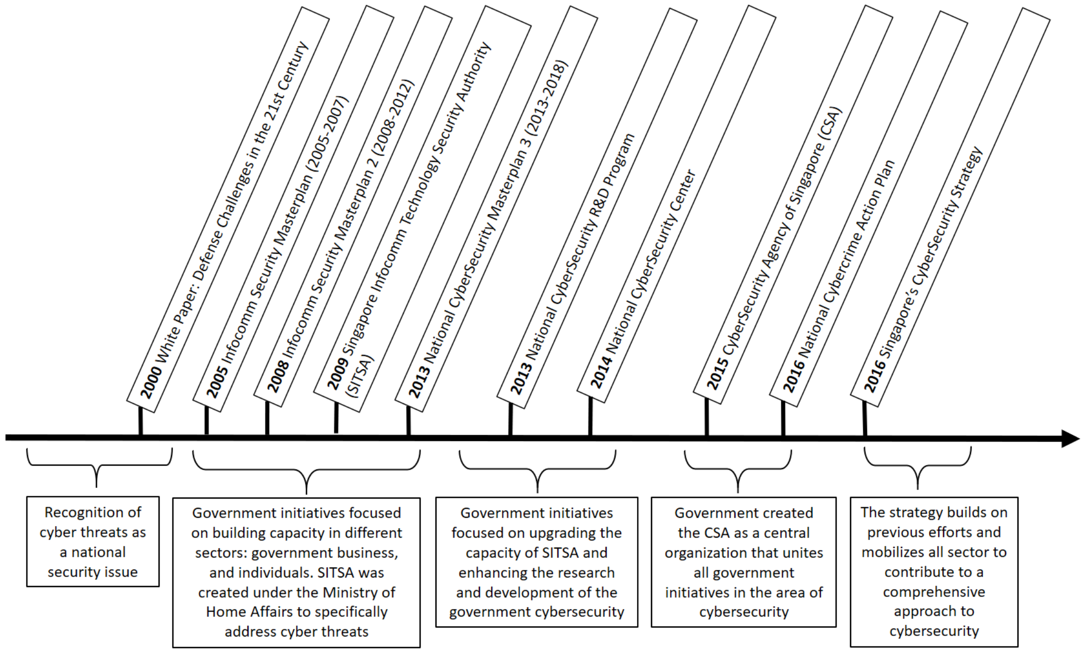
2012 Hacker TibitXimer downloads an estimated 3 million Verizon customer entries, leaking 10% of them (IMDA, 2017a)

2013 A DDoS attack targets Spamhaus, taking it offline for two days (IMDA, 2017a)

2013 A malicious third party infected Bit9's customers after the firm failed to install its own product on its network computers (IMDA, 2017a)

1.2 Main Policy Documents: Key Shifts in Strategy

Diagram SG2: Timeline of Policy Events and Trends[130]



2000 White Paper: Defense Challenges in the 21st Century

2005 Infocomm Security Masterplan (2005-2007)

2008 Infocomm Security Masterplan 2 (2008-2012)

2009 Singapore Infocomm Technology Security Authority (SITSA)

2013 National CyberSecurity Masterplan 3 (2013-2018)

2013 National CyberSecurity R&D Program

2014 National CyberSecurity Center

2015 CyberSecurity Agency of Singapore (CSA)

2016 National Cybercrime Action Plan

2016 Singapore's CyberSecurity Strategy

Recognition of cyber threats as a national security issue

Government initiatives focused on building capacity in different sectors: government business, and individuals. SITSA was created under the Ministry of Home Affairs to specifically address cyber threats

Government initiatives focused on upgrading the capacity of SITSA and enhancing the research and development of the government cybersecurity

Government created the CSA as a central organization that unites all government initiatives in the area of cybersecurity

The strategy builds on previous efforts and mobilizes all sector to contribute to a comprehensive approach to cybersecurity

[130] No clear distinction between infocomm security and cyber security was presented in any government document.

1.3 Organizational structures: key parameters

Singapore's approach to cybersecurity has involved at least three government agencies since the development of its strategy in 2005. The Ministry of Information and Communications was initially tasked to counteract cyberthreats through its operational agency, the Info-communications Development Authority (IDA). The IDA was also responsible for developing the first two versions of Singapore cyber strategy. The mandate to address cyberthreats was then centralized to the Ministry of Home Affairs, particularly the Singapore Infocomm Technology Security Authority, which was established in 2009.This system changed in 2015, when the Cyber Security Agency (CSA) of

Singapore's Cyber Security Agency (CSA) was created under the Prime Minister's Office to coordinate all aspects of cybersecurity within Singapore (Cyber Security Agency [CSA], 2016). The CSA became the lead organization that directed all government cybersecurity initiatives from the strategic to the operational levels of engagement. In the current system, the Singapore Police Force, through its newly created Cybercrime Command, handles law enforcement cyber issues while the Singapore Armed Forces SAF's under the auspices of the Ministry of Defense coordinates with the CSA in to responding to defense and national security issues.

Whereas the CSA is the main coordinating agency, the MINDEF has played an increasing active role in Singapore cybersecurity landscape created a Cyber Defense Operations Hub in 2013. This unit aims to improve the SAF's threat detection and analysis and reinforce network defense against emerging cyberthreats (Ministry of Defense, 2017). More recently it has also developed a Defense Cyber Organization (DCO) that is mandated to "oversee policies, capability development and implementation to monitor and defend" (Ministry of Defense, 2017) the computer networks of the Ministry of Defense and the SAF from cyberthreats. The impetus for this new military organization is the "significant growth in the risk of cyberthreats against countries, in particular, the increase in threats towards the military and the networks of defense industry and military related organizations" (Ministry of Defense, 2017).

1.4 Context/Analysis: key national trends

Singapore is a small highly developed state that was established as a republic after gaining independence from the United Kingdom in 1965 (Carpenter, 2008). It has a global reputation for technological advancement and has been resourceful in advancing its strategic interests by employing a combination of foreign policy tools to adapt to a rapidly changing strategic environment in the Asia-Pacific Region. The state is located adjacent to Malaysia and Indonesia, both of which contribute to the state's insecurity because of historical disputes as well as tensions over natural resources such as water, air quality, and airspace (Heng, 2013; Heilmann, 2015). In this regard, Singapore's continued apprehension with its neighbors contributes to its motivation to develop and maintain a strong military force relative to other states in the region.

Singapore is fixated with overcoming the strategic constraints imposed by its limited natural resources as well as small territory. The state compensates for these challenges by developing power projection capabilities that are anchored on advanced technology. Despite its limited personnel, the Singapore Armed Forces (SAF) is the most advanced military force in Southeast Asia. Singapore's sustained investment in Revolution of Military Affairs-critical areas such as precision weapons, command, communications, and computer-processing (C4) and intelligence, surveillance, and reconnaissance (ISR) has in enhanced its capacity to respond to regional threats independently and achieve a level of interoperability with powerful strategic partners such as the United States (Huxley, 2004).

On the hand, Singapore soft power projection is focused on building Smart Nation and establishing itself as the most highly networked state in the world (Baller, et al., 2016). The Smart Nation Platform (SNP) is the state's national effort to support a better quality of life through extensive and systematic use of technology to empower all members of Singaporean society and allow the state to compete with the global leaders in technology and innovation (Lee, 2014). Indeed, the SNP is Singapore's attempt at "virtual enlargement" or increasing its significance and influence through technological advancement (Chong, 2010). Moreover, projecting Singapore as a networked society is an indirect source of soft power that the state has taken advantage of because it solidifies its reputation as a leading financial and technology hub in the Asia-Pacific region.

The strategic use of network technologies for power projection has made Singapore increasingly vulnerable to network intrusions thereby escalating cybersecurity as a critical national security issue. In this sense, the state implemented a several interlinked cyber strategies that have contributed to strengthening different sectors of society during the last 13 years. This systematic and comprehensive approach to cybersecurity has enabled Singapore to develop an adaptable strategy that can respond to the multifaceted cyberthreats perpetrated by evasive actors.

2. Current cybersecurity policy

2.1 Overview of key policy documents

2.1.1 Infocomm Security Master Plans

Singapore's first Infocomm Security Masterplan (MP1) was implemented from 2005 to 2007. MP1 defined the overarching plan in the state's continued national efforts to strengthen cybersecurity and focused on protecting the government networks. Introduced in 2005, MP1 was a result of extensive private and public sector input with the objective of increasing the resilience of national critical infrastructure from cyber-intrusions and to maintain a secure environment for government, businesses and individuals. The MP1 identified six strategies to secure state's information communications environment: (i) securing the individuals, (ii) securing the private sector, (iii) securing the public sector, (iv) developing national capability, (v) cultivating technology and R&D, and (vi) securing national infrastructure (Infocomm Media Development Authority [IMDA], 2017).

Singapore's second Infocomm Security Masterplan (MP2) was implemented from 2008 to 2012. It was anchored on the achievements of MP1 and focused on protecting the critical infocomm infrastructure and services that supported Singapore's economy from cyber-incidents, thereby improving the confidence of investors in choosing the state as a strategic and secure location for their investments. Developed through a multiagency effort, MP2 was built on the collaboration between public, private and people sectors to secure Singapore's digital environment. In this sense, four strategic thrusts have been identified to support MP2's aim of achieving high resilience and availability of the nation's infocomm infrastructure and services: (i) harden national infocomm infrastructure and services, enhance infocomm security competencies, (iii) cultivate vibrant infocomm security ecosystem, and (iv) increase international collaboration (IMDA, 2017a).

Singapore's third master plan, the National Cyber Security Masterplan (NCSM2018), has been in effect since 2013 to and is scheduled to expire in 2018. The NCSM2018 builds on the work completed by previous master plans and brings Singapore's infocomm security to the next level of maturity and sophistication. Whereas MP1 focused on securing government networks and MP2 concentrated on protecting critical infocomm infrastructures, the NCSM2018 extended the efforts of the state to cover the wider information communications ecosystem to include businesses and individuals (IDMA, 2017b).

Three strategic imperatives underpin NCSM2018. The first imperative is to enhance the resilience of Critical Information Infrastructures (CIIs) to deal with sophisticated incidents. This imperative is undertaken by boosting cross-sector response to mitigate prevalent cyber-incidents. More specifically, the government works closely with critical sectors on security exercises, assesses critical infrastructure for vulnerabilities, “upgrading existing detection and analysis capabilities, and strengthening preventive and recovery measures at the Whole-of-Government level” (IDMA, 2017b).

The second imperative is to increase efforts to promote adoption of infocomm security measures among individuals and businesses. Small and medium-sized enterprises are often targets of cyber-intrusions are being used as conduits to attack higher-value targets in their supply chain. In this context, existing efforts will be reinforced to raise infocomm security awareness and adoption among businesses and individuals in Singapore. The third imperative is to develop a pool of infocomm security experts to address the shortage of cybersecurity professionals. There is an urgent need to explore new initiatives to increase the volume and capacity of cybersecurity professionals in Singapore. To manage this situation, existing initiatives will focus on pushing further to develop human capital within Singapore's infocomm industry through the implementation of the National Cybersecurity R&D Program and Company-Led Training (CLT) Program as well as the establishment of a training facility for developing and retraining experts: the DigiSAFE Cyber Security Centre (IDMA, 2017b).

2.1.2 Singapore's Cybersecurity Strategy 2016

The Cybersecurity Strategy 2016 is the most recent document that explains Singapore's approach to managing cyberthreats. It is the most comprehensive document released by Singapore to date because it draws on all the substance of the previous master plans and integrates the key measures in one coherent strategy.

The primary objective of the strategy is to create a resilient and trusted cyber environment to enable Singaporeans to realize the advantages of technology. This objective is pursued through four pillars that define the strategy. The first pillar focuses on strengthening the resilience of Singapore's CII. This is pillar is based on the logic that despite Singapore's comprehensive efforts to secure its networks, it is still vulnerable to cyber-intrusions. In this sense, resilience is critical to maintaining a robust cyber strategy. The second pillar concentrates on creating a safer cyberspace where threats are systematically mitigated through the shared initiatives between different sectors of society. This pillar builds on Singapore's previous efforts that centered on securing government networks, private networks, and promoting cyber hygiene practices among individuals.

The third pillar aims to develop a vibrant cybersecurity ecosystem by building a highly capable information technology workforce as well as Institutes of Higher Learning to harness cybersecurity R&D. A dynamic cybersecurity ecosystem is essential for Singapore to position itself at the global forefront of innovation in cybersecurity research. The fourth and last pillar is to maintain strong international partnerships in cybersecurity. This pillar is based on Singapore's assessment of its limitations both in resources and expertise when addressing cybersecurity issues. This initiative is accepts that Singapore cannot sufficiently counter cyberthreats without cooperating with different members of the international community.

2.2 National cybersecurity strategy: fields, tasks, priorities

A further examination of the four pillars of Singapore's Cybersecurity Strategy reveals the development of comprehensive measures that contribute to a "resilient and trusted cyber environment." The first pillar, building resilient critical information infrastructures, is enforces through five measures. Firstly, by implementing a Critical Information Infrastructures Protection Program that establishes a robust and systematic cyber risk management processes across all critical sectors. Secondly, by mounting multi-sector cybersecurity exercises to test cooperation across multiple sectors and address inter-dependencies during major cyber-intrusions. Thirdly, by capacitating the National Cyber Incident Response Team (NCIRT) and the National Cyber Security Centre (NCSC) will also be enhanced to improve responsiveness. Fourthly, by passing the Cybersecurity Act to give the Cyber Security Agency of Singapore (CSA) greater authority to monitor and prosecute individuals and organization that threaten to disrupt CII (CSA, 2016).

The second pillar aims to create a safer cyberspace though the collective effort of government, business and individuals. The government aims to pursue this pillar by firstly implementing its National Cybercrime Action Plan that was released in 2016. Secondly, the government will work with global institutions, other governments, industry partners and Internet Service Providers to identify and reduce malicious traffic on our Internet infrastructure. Thirdly, the government will enable communities and business organization through public-private partnerships that focus on developing knowledge about cybersecurity issues and promoting the adoption of good practices (CSA, 2016).

The third pillar centers on developing a vibrant cybersecurity ecosystem. This involves three measures. The first is developing a skilled workforce that entails collaboration with industry partners and higher education institutes to grow the workforce and encourage existing cybersecurity professionals to deepen their skills. The second is to develop strong companies and nurture local start-ups to ensure that the most appropriate solutions are available locally. Singapore is traditionally strong in areas such as financial and information communications services therefore, cybersecurity firms have the opportunity to develop exportable solutions. The third measure is fostering partnerships between academia and industry so as to harness cybersecurity R&D in a more targeted manner to deliver effective solutions (CSA, 2016).

The fourth and last pillar of the strategy is to forge strong international partnerships. The government intends to follow through with this pillar by actively cooperating with the international community, particularly Association of Southeast Asian Nations (ASEAN), to address transnational cybersecurity and cybercrime issues. In this regard, Singapore will champion capacity-building initiatives in cybersecurity, and facilitate exchanges on cybernorms and legislation. The focus is on facilitating international consensus, agreement, and cooperation to make cyberspace a safer and more secure place for all (CSA, 2016).

2.3 National cyberdefense strategy: fields, tasks, priorities

Singapore does not have a dedicated cyberdefense strategy but its initiatives in this area are subsumed with Cybersecurity Strategy 2016 and consistent with the state's Total Defense strategy, which requires all sectors of society to develop a robust and proactive capability to respond to national security threats (CSA, 2016). In this context, the Singapore's efforts to counter cyber-intrusions are manifested in two defensive measures discussed in the Cybersecurity Strategy 2016. One defensive measure is to strengthen the resilience of its critical information infrastructures. Singapore's approach towards cyberdefense is to assume that there will be successful cyber-intrusions against its networks. A decisive response to these intrusions requires reliable recovery plan that enables for "timely response and ground initiative at the local level" in concert with effective coordination and strategic support at the national level (CSA, 2016). Another measure that is defense-oriented is to boost the government's capacity and capability to combat cybercrimes and to minimize the effectiveness of cyberthreats in general. In this sense, Singapore's focus on enhancing its investigative capabilities, specifically in the areas of incident response, network detection, malware analysis and digital forensics is central to its objective of building a safer cyberspace.

There are two main agencies that manage the cyberdefense initiatives of Singapore. The CSA as discussed in the previous section, is the lead government organization that coordinates all government initiatives relating to cybersecurity. This includes the protection of critical sectors such as energy, water, and banking and ensuring effective coordination and deployment in response to persistent cyberthreats (CSA, 2018). A recently established and more specialized agency that is a key for cyberdefense is the Defense Cyber Organization (DCO). The DCO compliments the efforts of the CSA by protecting all the networks and systems within the defense sector including the Singapore Armed Forces, Ministry of Defense, Defense Science Technology Agency, DSO National Laboratories, Defense Industry and other MINDEF-Related Organizations (Ministry of Defense, 2018).

2.4 Context/Analysis: key policy principles

Singapore's efforts in securing its networks and systems are mainly directed by civilian government leaders working with four government offices: Prime Minister's Office, Ministry of Communications and Information, Ministry of Home Affairs, and the Ministry of Defense. Even with this arrangement, the military still figures prominently in the state's cybersecurity efforts. There are two indicators that support this point. First, Singapore is the first state to officially publicize that it is establishing a cyber command in the region. Second, despite the clear distinctions between the operational mandates of the CSA and DCO, the same chief executive who was formerly a general with the SAF, manages the two government agencies.

As discussed in the previous sections, Singapore's strategy for protecting its interests in cyberspace has evolved through four phases. These interconnected phases are documented in three previous master plans and a culminating document that defines the state's current cybersecurity strategy. The key initiatives presented in these documents are focused on defense and resilience with the first three master plans implemented to strengthen the resilience of the government, critical information infrastructures, business and individuals against cyber-intrusions as well as enhance the defensive capabilities of specific government agencies. Singapore's current Cyber Security Strategy integrates the main initiatives of the previous master plans and presents a more cohesive strategy that reinforces the resilience of CII and proactively counters cyberthreats.

While Singapore is concentrated on enhancing its cyber capabilities, there is no mention of offensive measures or computer network attacks as part of its cybersecurity strategy in an of its policy documents. Indeed, the state's version of a military cyber command is clearly designated as a defensive organization with the objective of protecting the networks of the Ministry of Defense, Singapore Armed Forces and other defense-related organizations. There are two reasons for the absence of offensive measures in Singapore's strategies. First, the state's defense policy is constructed on the foundations of deterrence and diplomacy so any representation of offensive cyber capabilities in policy documents may contradict Singapore's foreign policy (Matthews and Yan, 2007). Second, while deterrence is an integral part of Singapore defense policy, it is not clear that publicizing the existence of offensive cyber capabilities can actually deter adversarial states and non-state actors.

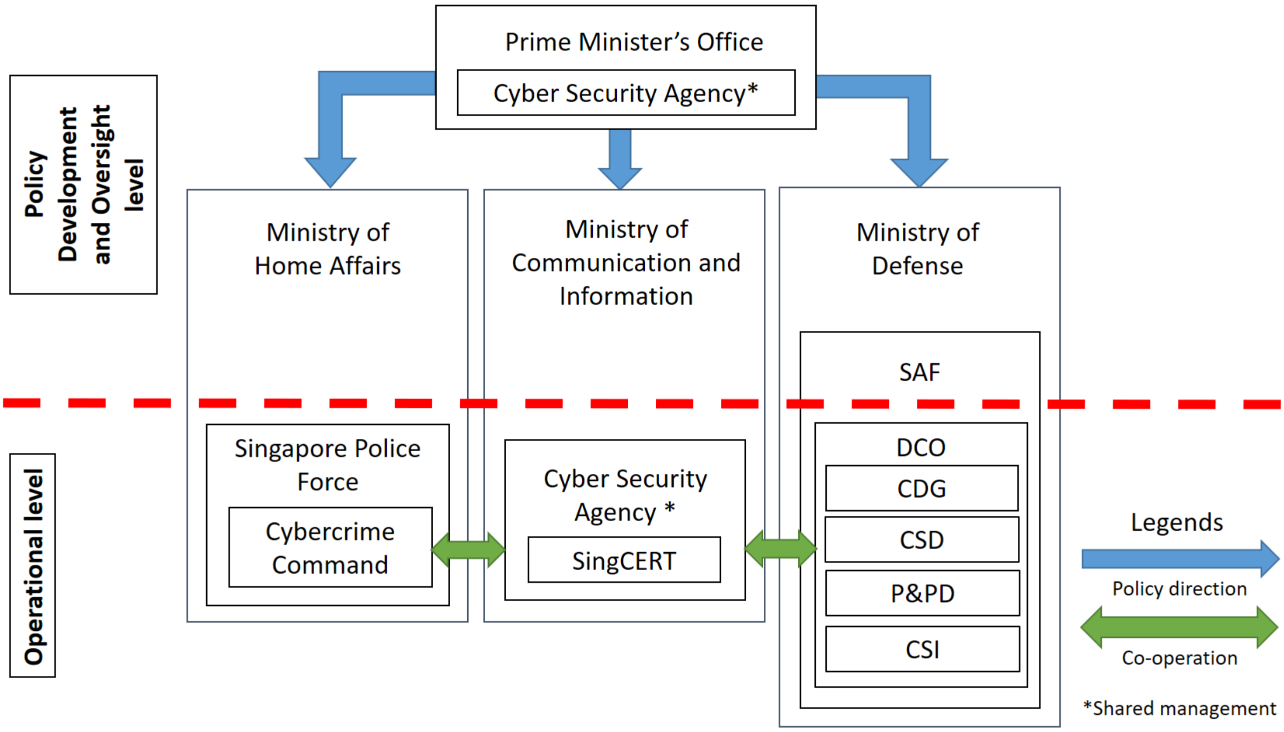
A consistent theme across all policy documents is the need to continuously innovate to maintain the technological advantage over other states in the region. Continuous innovation is therefore necessary in developing "cutting-edge" cyber capabilities that will enable a safer cyberspace and consequently secure a better future for Singaporeans.

3. Current public cybersecurity structures and initiatives

3.1 Overview of national organization framework

Diagram 3 below provides a graphical representation of Singapore's cybersecurity apparatus.

Diagram SG3: Oversight Organigram



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

3.2.1 The Cybersecurity Agency

The CSA was established in April 2015 to consolidate all the state's efforts in countering cyberthreats. The CSA functions under the Prime Minister's Office but is directed administratively by the Ministry of Communications and Information (MCI). Its mandate is to supervise cybersecurity strategy, operation, education, outreach, and ecosystem development in Singapore. The CSA coordinates cybersecurity initiatives at all levels of government. It has inherited the policy functions (development of master plans) from the Infocomm Development Authority (IDA), as well as the operational and technical functions from the Singapore Infocomm Singapore Computer Emergency Response Team (SingCERT) and the Singapore Infocomm Technology Security Authority (SITSA).

In implementing Singapore's cyber strategy, the CSA cooperates with the Singapore Police Force (SPF) and the SAF. The SPF is central to Singapore cybersecurity efforts given that it is the primary government agency designated to respond to cybercrimes.

3.2.2 SPF Cybercrime Command

The Ministry of Home Affairs established the Cybercrime Command as a unit within the Criminal Investigation Department of the Singapore Police Force (SPF) in December 2015 (CSA, 2016). The purpose of the Command is to enhance its agility and effectiveness of the SPF in responding to cybercrimes. The Command integrates all SPF's cyber-investigation, forensics, intelligence and crime prevention capabilities within a single unit. This enables the SPF to cooperate more effectively with other government agencies, industry, and the public, in developing robust responses to the constantly evolving nature of cybercrime.

In terms of operations, the Cybercrime Command oversees Cybercrimes Response Teams based in every Police Land Division or field offices. These teams assist investigation officers in responding to incidents reports by collecting processing digital evidence, conducting forensic analysis of digital devices. In terms of education, the Cybercrime Command develops the curriculum for SPF's specialized cybercrime investigation training modules for new police officers. Through these modules, SPF investigation officers are capable of specialized skills like email header analysis and the process of recognizing, collecting and preserving digital evidence (Ministry of Home Affairs, 2016).

The SPF cooperation with the CSA is manifested through the implementation of National Cybercrime Action Plan (NCAP). There are four areas where the SPF and the CSA work together in combating cybercrimes. The first is public awareness through public education about cyberthreats. The second is developing the capacity to investigate complex cyber-incidents and sharing cybersecurity expertise among government agencies. The third is strengthening legislation and the criminal justice framework by amending existing laws and improving regulatory frameworks. The last area is enhancing international engagements through increasing cybercrime awareness in the private sector as well as advocating for regional and global cooperation in the area of cybersecurity (Ministry of Home Affairs, 2016).

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

The MINDEF established the Defense Cyber Organization in 2017, consistent with the national initiatives to create a secure and resilience infocomm environment. The DCO has two core missions. The first is to lead the efforts in securing networks and systems across the Defense Sector, particularly and to overcome any cyber-intrusions definitively, maintaining the continuity of the operations of defense and military institutions. The DCO is divided into four formations across the MINDEF – the Cyber Security Division (CSD), Policy and Plans Directorate (P&PD), the Cyber Security Inspectorate (CSI), and the Cyber Defense Group (CDG).

The Cyber Security Division is the operational arm of the DCO. It provides regular cybersecurity oversight in the different agencies within the Defense Cluster and responding to any attacks that may occur. The Policy and Plans Directorate designs the overall cyberdefense capability development plan for the Defense Cluster. The Cyber Security Inspectorate helps strengthen the Defense Cluster's counter measures through the conduct of vulnerability assessment exercises and ensuring that each sector adheres to established cyberdefense policies. The Cyber Defense Group (CDG) is specifically designated to protect the SAF's capacity to execute cyber-operations against adversaries. The creation of a CDG enhances the SAF's robust and resilient military networks and systems against cyberthreats. (Ministry of Defense, 2017).

The DCO cooperates with the CSA but there is currently no government document that provides any explicit discussion about cooperation between the two agencies but there are at least two indications of collaboration. The first is the reference to Total Defense in Singapore's Cybersecurity Strategy. Total Defense is a comprehensive framework that guides the entire state in implementing a holistic response to national security threats and challenges. The DCO contributes to Total Defense through the Military Defense pillar of the framework while. The CSA contributes predominantly to the Economic Defense and Civil Defense pillars of the Total Defense framework. More specifically, the DCO focuses on protecting defense and military networks while the CSA focuses on civilian networks. The second indication is the leadership of both government agencies. It is not a coincidence that the same chief executive, who was formerly a general with the SAF manages the DCO and CSA. The overlap in leadership enables less friction in the coordination efforts between key civilian and military agencies in countering cyberthreats.

3.4 Context: key public organizational framework

Singapore's governance structure for managing cybersecurity issues is small and highly centralized, consistent with the state's wider political structure. The Prime Minister's Office (PMO) coordinates all the government's cybersecurity initiatives of the state through the CSA, in close coordination with the Ministry of Defense and the Ministry of Home Affairs. In terms of operations, the CSA is tasked with the overall defense of government networks through the Singapore Computer Emergency Response Team (SingCERT). The Ministry of Defense supports the CSA by protecting all defense and military networks from high-level cyber-intrusions while the Ministry of Home Affairs reinforces the operations of the CSA by monitoring criminal activities online. There are at least two implications of Singapore's centralized government structure for cybersecurity.

One implication relates to Singapore's strategic limitations as a small state with limited materials resources. The state's inherent lack of materials resources and political influence makes it difficult to advance its interests in a competitive geopolitical environment such as the Asia-Pacific Region (Chong, 2012; Burton, 2013). In adapting to these limitations, the state needs decisive and robust responses to all national security threats particularly against Critical Information Infrastructures that reinforce its primary objective of becoming the leading technological hub in the region.

Another implication relates to Singapore's strategic culture that previous studies characterize as "insecure" and shaped by a "siege mentality" (i.e. defensive or paranoid) (Ganesan, 2005; Ho, 2009; Tan, 2012). In this sense, the preference for centralization is influenced by the state's insecurity from its limited capacity to respond to national security threats. For instance, this strategic predicament demands a more integrated and faster response to counteract threats such as espionage, sabotage and crimes. For instance, cybercrimes are a source of disruption and insecurity because they can involve governments of hostile states and undermine one of the state's core national interests: robust economic growth.

Singapore's preference for a centralized governance structure, where authority is concentrated on the Prime Minister's Office raises some implications for the state's approach in managing cybersecurity issues. A centralized governance structure can contribute to a robust, less bureaucratic response to cyberthreats however, it can also contribute to exploitation if the government uses the authority to implement policies that regulates Internet use and content. For instance, while the state does not implement strong Internet filtering measures, it "employs a combination of licensing controls and legal pressures to regulate Internet access and to limit the presence of objectionable content and conduct online" (Deibert, et al., 2011, pp. 364-367). These policies are typically utilized to monitor the information ecosystem from potential national security threats however, these can also be utilized to pinpoint dissidents that challenge the power and authority of the state's political leaders (Rodan, 1998; George, 2007).

There is no evidence to suggest that the government agencies constrained by the lack of material resources. Indeed, Singapore is looking to allocate around 10% of its budget for information and communication technologies for cybersecurity, consistent with the practice in other states with considerable cyber capabilities such as Israel and South Korea (Ibrahim, 2015). More significantly, Singapore typically invests more resources for national security than most states in the region, spending around 3.9% (regional average is 1.8%) of its GDP from 2000 to 2016 just for national defense (Stockholm International Peace Research Institute [SIPRI], 2016).[131]

[131] North Korea, Turkmenistan, and Uzbekistan were excluded from the estimate because of the lack of data on their respective military expenditures.

4. Cyberdefense and Cybersecurity partnership structures and initiatives

4.1 Public-Private cyberdefense partnerships

Singapore's initiatives in cyberdefense are implemented within its broader cybersecurity strategy, as discussed in the previous sections. The significance of establishing public-private partnerships in cybersecurity is discussed specifically under the third pillar of its strategy, developing a vibrant cybersecurity ecosystem. A key objective of the third pillars to "extend Singapore's advantage through strong local companies" (CSA, 2016). The focus of this initiative is to develop local cybersecurity leaders who can compete globally in strategic areas of interest and public-private partnerships are useful schemes to achieve this objective.

One example of a public-private partnership program is the Partnership for the Advancement of the Cybersecurity Ecosystem (PACE) program, which was initiated by the CSA in 2016. The PACE program has contributed to the cybersecurity efforts of Singapore because it co-develops customized solutions with industry partners that raise cybersecurity posture of the state while reinforcing workforce skills development (CSA, 2016). Another example is Singapore's efforts to boost its R&D capacity by collaborating more closely with academia and industry to address real-world problems in a more targeted manner, and move research products faster from the laboratory to the market. This objective is realized through new cutting-edge R&D facilities established through the collaboration between universities and industry partners such as the Cyber Security Laboratory of ST Electronics and Singapore University of Technology and Design (CSA, 2016).

4.2 International cyberdefense partnerships

Singapore's international partnerships in cybersecurity are oriented towards on strengthening cooperation with ASEAN partners as well as maintain several bilateral ties with capable states such as France, Netherlands, United Kingdom, and United States. The cooperation of ASEAN partners is central to Singapore's cybersecurity efforts because it aims to become the leader in all aspects of cybersecurity in the region. In this context, the state intends to pursue a leadership role by pursuing three measures. First, Singapore plans to work with ASEAN partners to strengthen platforms and procedures for cyber-incident reporting and response, with the objective of coordinating the regional approach to cybercrime.

Second, Singapore intends lead international and regional efforts in building capacity in operational, technical, legislative, cyber policy and diplomatic areas of cybersecurity. These initiatives are realized through organize workshops, seminars and conference such as the IoT Asia and the Singapore Cyber Security R&D Conference that seek to advance cooperation and build capabilities in these aspects. Third, the state expects to facilitate exchanges on cybernorms and legislation through the annual Singapore International Cyber Week (SICW). The objective to this measure is to "catalyze, stimulate and promote" debates on strategic cyber issues including the advancement of norms, development of cyber policies and legislation, deterrence in cyberspace, and cooperation against cybercrimes (CSA, 2016).

Aside from regional initiatives, Singapore has actively developed international partnerships in with a number of leading states to enhance its operational and technical capacity to respond to secure its interests in cyberspace. For instance, the CSA and its French counterpart, the Agence Nationale de la Sécurité des Systèmes d'Information signed a Memorandum of Understanding last 2015 to strengthen national cyber capabilities "through more regular bilateral exchanges, sharing of best practices and efforts to develop cybersecurity expertise" (CSA, 2015). In 2016, Singapore signed another Memorandum of Understanding with the United States "to formalize their commitment to work together in building a secure and resilient cyberspace through cybersecurity cooperation" (CSA, 2016a). The agreement covers cooperation in crucial areas including regular exchanges between Computer Emergency Response Teams, sharing of best practices in cyber-incident response and sharing best practices in protecting CIIs.

4.3 Cyberdefense awareness programs

Singapore's efforts in building awareness about cybersecurity issues is generally led by the government but with strong support from the private sector. Cybersecurity awareness is a key theme discussed within the second pillar of state's cyber strategy: creating a safer cyberspace. The significance of awareness is emphasized through several measures, two of which are combating cybercrime and promoting collective responsibility for cybersecurity issues. A key principal in preventing individuals and organizations from becoming victims of cybercrimes is strengthening efforts "to educate the public and boost awareness of cyber hygiene" (Ministry of Home Affairs, 2016). This is realized through the SPF's information campaign on cybersecurity, which involves systematic dissemination of "cybercrime prevention messages with the public via various media platforms, such as television, newspapers, social media, text messages and posters at public transport nodes and lifts in public housing blocks" (CSA, 2016). Focusing on the community level, the

SPF, through its Public Cyber-Outreach & Resilience Program, uses "behavioral insights" to encourage the general public to assume good cyber hygiene practices (CSA, 2016).

Meanwhile, promoting collective responsibility for cybersecurity issues involves two initiatives. The first is making cybersecurity a priority for businesses by recognizing and treating cyber risks as important business risks. The second is taping government cybersecurity expertise "to improve their members' understanding of cybersecurity issues and encourage adoption of good practices" (CSA, 2016). The most elaborate project to date that incorporates these initiatives has been the Cyber Security Awareness Alliance, a coalition of government agencies, private enterprises, and non-profit organizations that was established by the IDA in 2008 and now co-chaired by the CSA. The principal aims of the alliance are twofold: to "build a positive culture of cybersecurity in Singapore" and to "promote and enhance awareness and adoption of essential cybersecurity practices for both the private and public sectors." Since its formation, the Cyber Security Awareness Alliance has reached out to various audiences through exhibitions, online information campaigns (https://www.csa.gov.sg/gosafeonline), and talks (CSA, 2019).

4.4 Cyberdefense education and training programs

The Singaporean Government has not disclosed details on training and R&D programs that focus exclusively on enhancing any type of government cyber capabilities. Existing efforts concentrate on strengthening the cybersecurity capacity of all sectors of society through a constant collaboration through research and development. Aside from the National Cybersecurity R&D Program (Section 2.1.3) and PACE Program (Section 4.1) discussed in previously, another key initiative for education and training is the Singapore Cybersecurity Consortium, which is specifically designed to boost the "engagement between industry, academia and government agencies to encourage use-inspired research, translation, manpower training and technology awareness in cybersecurity" (Singapore Cyber Security Consortium, 2018). The Consortium is funded by the Prime Minister's Office and anchored at the National University of Singapore.

4.5 Cyberdefense research programs

Singapore's primary organization for military research and development in the area of cybersecurity is the Defense Science & Technology Agency (DSTA). The DSTA is a statutory board under the Ministry of Defense and was developed to harness science and technology, and provide technological and engineering support necessary to sustain the defense and national security needs of Singapore (Defense Science & Technology Agency [DSTA], 2018). DSTA's cybersecurity program explores on three general themes: cyber policy, network defense, and diverse cyber solutions.

In terms of policy, the DSTA is involved in the development of a National Cybersecurity R&D roadmap that aims to enhance the security, reliability and resiliency of computer networks and other computer systems that are critical to Singapore. The organization main contribution in this effort is to guide and support a working group composed of key government agencies to determine their requirements in the area of cybersecurity. These requirements were then congregated into practical research challenges that academia and industry can further study and develop prototypes (DSTA, 2016).

In the area of network defense, the DSTA has at least three initiatives. First, the agency developed a technique and a prototype to detect sophisticated malware. The prototype was tested successfully against advanced malware such as Stuxnet and TDSS (DSTA, 2016a). Second, the agency developed measures to secure information exchange and to prevent data leaks. This was implemented through a modification of "the cryptographic algorithm of the encryption process to strengthen the encrypted information against cryptographic attacks" (DSTA, 2016b). Third, the agency developed a malware analyzer that protects its network and computers against threats that are sent through emails. The tool "analyses email attachments for malicious behavior and performs analytics to detect cyberthreats that may be unknown previously" (DSTA, 2016c).

The agency also contributes to developing a range of cyber solutions to protect the military's computer networks and assets such as air defense systems, unmanned aerial vehicles and the Advanced Combat Man Systems. These solutions are crucial for the Singapore Armed Forces to sustain technological superiority over its neighbors and maintain interoperability with military forces of more powerful states such as the United States of and the United Kingdom (DSTA, 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 SG4: Spectrum of Centralization vs Decentralization of policy development and management

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

5.2 Civilian vs defense posture and oversight

Diagram SG5: Spectrum of Civilian-Defense cybersecurity posture and oversight

Civilian oversight -----X-- Defense

5.3 Offensive vs defensive capabilities

Diagram SG6: Spectrum of Offensive vs Defensive cyberdefense capabilities

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

6. Annex 2: Key definitions

Term	English
Critical Information Infrastructure	Computer systems directly involved in the provision of essential services to the state.
Cyber hygiene	Steps that users can take to protect themselves online. Examples of cyber hygiene practices include using a firewall,
Masterplans	A set of measures developed and implemented by the Singaporean Government from 2005 to 2018 to secure the state's digital environment by systematically strengthening the cybersecurity capabilities of the public sector, private sector, and individuals.
Smart Nation	Smart Nation is a concept that denotes a national effort to build a nation-state where people live meaningful and fulfilled lives, enabled seamlessly by technology, offering exciting opportunities for all.
SingCERT	The Singapore Computer Emergency Response Team (SingCERT) responds to cybersecurity incident for its Singapore constituent. It was set up to facilitate the detection, resolution and prevention of cybersecurity-related incidents on the Internet.
Total Defense	A concept introduced by the Singaporean Government in 1984 to involve every Singaporean in playing a part, individually and collectively, to build a strong, secure and cohesive nation. It involves all citizens of Singapore in the following five aspects: military defense, civil defense, economic defense, psychological defense and social defense.

7. Annex 3: Abbreviations

Abbreviation	English
ASEAN	Association of Southeast Asian Nations
CDG	Cyber Defense Group
CII	Critical Information Infrastructure
CSA	Cyber Security Agency
CSD	Cyber Security Division
CSI	Cyber Security Inspectorate
DCO	Defense Cyber Organization
DSTA	Defense Science & Technology Agency
IDA	Info-communications Development Authority
IMDA	Infocomm Media Development Authority
MINDEF	Ministry of Defense
NCAP	National Cybercrime Action Plan
NCIRT	National Cyber Incident Response Team
NCSC	National Cyber Security Centre
P&PD	Policy and Plans Directorate
SAF	Singapore Armed Forces
SFP	Singapore Police Force
SingCERT	Singapore Computer Emergency Response Team
SITSA	Singapore Infocomm Technology Security Authority

8. Bibliography

Baller, S., Dutta, S., & Lanvin, B. (2016). The Global Information Technology Report 2016. Geneva, Switzerland: World Economic Forum.

Burton, J. (2013). Small States and Cyber Security: The Case of New Zealand. Political Science, 65(2), 216-238. doi: 10.1177/0032318713508491

Carpenter, W. M. (2005). Singapore: Stability and Prosperity, In William M. Carpenter and David G. Wiencek (Eds.) Asian Security Handbook: Terrorism and the New Security Environment, 3rd ed. (259-263) London & New York: M. E. Sharpe.

Chong, A. (2012). Singapore's Encounter with Information Warfare. In D. Ventre (Ed.), Cyber Conflict Competing National Perspectives (pp. 223-250). London, UK: ISTE, Ltd.

Chong, A. (2010). Small state soft power strategies: virtual enlargement in the cases of the Vatican City State and Singapore. Cambridge Review of International Affairs 23 (3), 383-405. doi: 10.1080/09557571.2010.484048

Chua, Alfred (2017, 28 February) Mindef hit by targeted cyber attack Retrieved from: https://www.todayonline.com/singapore/mindef-internet-system-hacked-personal-data-850-personnel-stolen

Deibert, R. Palfrey, J., Rohozinski, R. and Zittrain, J. (2011). Access Contested: Security, Identity, and Resistance in Asian Cyberspace. Cambridge, Massachusetts: MIT Press.

Ganesan, N. (2005). Realism and Interdependence in Singapore's Foreign Policy. London: Routledge.

George, C. (2007). Consolidating Authoritarian Rule: Calibrated Coercion in Singapore Pacific Review, 20 (2), 127-145.

Heng. Y. (2013). A Global City in an Age of Global Risks: Singapore's Evolving Discourse on Vulnerability Contemporary Southeast Asia 35 (3), 423-446. doi: 10.1355/cs-3e

Heilmann, D. (2015). After Indonesia's Ratification: The ASEAN Agreement on Transboundary Haze Pollution and Its Effectiveness As a Regional Environmental Governance Tool Journal of Current Southeast Asian Affairs, 34 (3) 95–121.

Ho, S. H. (2009). Hegemony of an Idea (Discussion Paper n° 5 - Note de recherche n° 5). Retrieved from: http://www.irasec.com/ouvrage43

Huei, Peh Shing (2014, October 3) Drawing the line between privacy and public interest Retrieved from: https://www.straitstimes.com/forum/readers-post/drawing-the-line- between-privacy-and-public-interest

Huxley, T. (2004). Singapore and the Revolution in Military Affairs In E. Goldman and T. Mahnken, The Information Revolution in Military Affairs in Asia (pp. 185-208) London: Palgrave Macmillan.

Lee, H. l. (2014, November 24) Launch of Smart Nation Initiative, Speech at Smart Nation Launch. Retrieved from: http://www.pmo.gov.sg/newsroom/transcript-prime-minister-lee-hsien-loongs-speech-smart-nation-launch-24-november

Liang, Lim Yan (2013, November 12) Hacker who calls himself 'The Messiah' charged with hacking; More being investigated Retrieved from: https://www.straitstimes.com/singapore/hacker-who-calls-himself-the-messiah-charged-with-hacking-more-being-investigated

Matthews, R. and Yan, N.Z. (2007). Small Country 'Total Defence': A Case Study of Singapore 7 (3), 376-395. doi: 10.1080/14702430701559289

Rodan, G. (1998). The Internet and Political Control in Singapore Political Science Quarterly 113 (1), 63-89.

Singapore Cyber Security Agency. (2019). About the Cyber Security Awareness Alliance. Retrieved from: https://www.csa.gov.sg/gosafeonline/content/cyber-security-awareness-alliance

Singapore Cyber Security Agency. (2018). Singapore Cyber Landscape 2017. Singapore: Cyber Security Agency.

Singapore Cyber Security Agency. (2016). Singapore's Cybersecurity Strategy. Singapore: Cyber Security Agency.

Singapore Cyber Security Agency. (2016a, August 3). Singapore Strengthens Partnership with the United States. Retrieved from: https://www.csa.gov.sg/news/press-releases/ singapore-us-mou#sthash.c20bI1f3.dpuf

Singapore Cyber Security Agency. (2015, May 18). CSA Signs First International MOU with France to Strengthen Cyber Security Collaboration. Retrieved from: https://www.csa. gov.sg/news/press-releases/csa-signs-first-international-mou-with-france-to- strengthen-cyber-security-collaboration#sthash.LQCV9Ehu.dpuf

Singapore Cyber Security Consortium (2018). About Us. Retrieved from: https://sgcsc.sg/ index.html

Singapore Defense Science & Technology Agency (2018, May 7). Overview. Retrieved from: https://www.dsta.gov.sg/about/overview

Singapore Defense Science & Technology Agency (2017, December 1). Cybersecurity Retrieved from: https://www.dsta.gov.sg/programme-centres/cybersecurity

Singapore Defense Science & Technology Agency (2016, November 16). Developing National Cybersecurity Roadmap. Retrieved from: https://www.dsta.gov.sg/programme-centres/cybersecurity/developing-national-cybersecurity-roadmap

Singapore Defense Science & Technology Agency (2016a, November 16). Detecting Advanced Malware. Retrieved from: https://www.dsta.gov.sg/programme-centres/cybersecurity/detecting-advanced-malware

Singapore Defense Science & Technology Agency (2016b, November 16). Securing Our Data. Retrieved from: https://www.dsta.gov.sg/programme centres/cybersecurity/ securing-our-data

Singapore Defense Science & Technology Agency (2016c, November 16). Guarding the Email Communication Channel. Retrieved from: https://www.dsta.gov.sg/programme-centres/cybersecurity/guarding-the-email-communication-channel

Singapore Infocomm Media Development Authority. (2017, November 3). Infocomm Security Masterplan. Retrieved from:https://www.imda.gov.sg/industry-development/programmes-and-grants/enterprises/infocomm security/initiatives/ infocomm-security-masterplan

Singapore Infocomm Media Development Authority. (2017a, November 3). Infocomm Security Masterplan 2. Retrieved from: https://www.imda.gov.sg/industry-development/programmes-and-grants/enterprises/infocomm security/initiatives/infocomm-security-masterplan-2

Singapore Infocomm Media Development Authority. (2017b, November 3). National Cyber Security Masterplan 2018: What you need to know Retrieved from: https://www. imda.gov.sg/infocomm-and-media-news/whats-trending/2014/12/national-cyber- security-masterplan-2018-what-you-need-to-know Singapore Ministry of Defence. (2018, October 4). Defense Cyber Organization. Retrieved from: https://www.mindef.gov.sg/web/portal/mindef/about-us/organisation/organisation-profile/defence-cyber-organisation

Singapore Ministry of Defence (2017, March 3). Fact Sheet: Next Gen SAF's New Cyber Command to Combat Growing Cyber Threat. Retrieved from: https://www.mindef. gov.sg/imindef/press_room/details. html?name=03mar17_fs2&date=2017-03-03#.WdN8DVtSyUk

Singapore Ministry of Home Affairs (2016). National Cybercrime Action Plan. Singapore: Ministry of Home Affairs.

Stockholm International Peace Research Institute (2016). Military Expenditure Database. Retrieved from: https://www.sipri.org/databases/milex

Tan, S. S. (2012). Faced with the Dragon: Perils and Prospects in Singapore’s Ambivalent Relationship with China. The Chinese Journal of International Politics 5 (3), 245–265, doi: 10.1093/cjip/pos012

Tham, Irene (2018, July 20) Personal info of 1.5m SingHealth patients, including PM

Lee, stolen in Singapore's worst cyber attack https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most

Tham, Irene (2017, May 16) WannaCry could have infected computers linked to some 500 IP addresses in Singapore Retrieved from: https://www. straitstimes.com/tech/wannacry-could-have-infected-computers-linked-to-some-500-ip-addresses-in-singapore

The United Kingdom

Robert S. Dewar
Center for Security Studies
ETH Zürich[132]

[132] Robert S. Dewar is now Head of Cyber Security at the Geneva Centre for Security Policy.

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 cyber risks 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 cyber risks 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 Programme 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 cooperates 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.

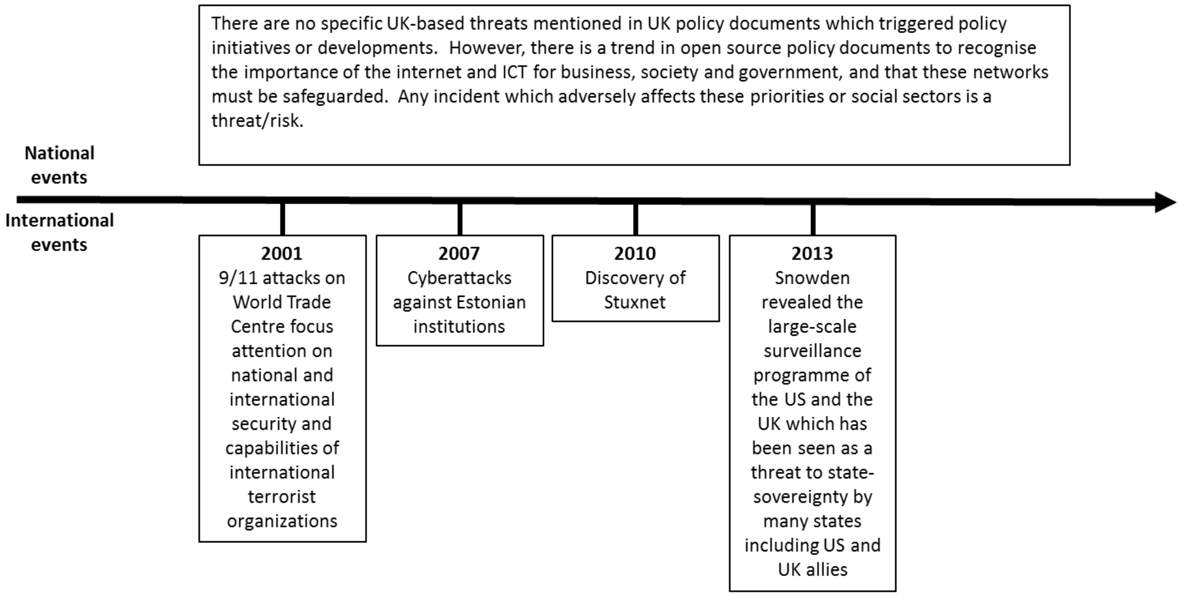
The UK actively promotes private sector partnership and involvement in cybersecurity (and by extension cyberdefense) provision, to the extent that it recognizes in policy that a significant portion of the UK's cybersecurity and defense tools and measures will be owned and operated by the private sector. 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



There are no specific UK-based threats mentioned in UK policy documents which triggered policy initiatives or developments. However, there is a trend in open source policy documents to recognise the importance of the internet and ICT for business, society and government, and that these networks must be safeguarded. Any incident which adversely affects these priorities or social sectors is a threat/risk.

National events

International events

2001 9/11 attacks on World Trade Centre focus attention on national and international security and capabilities of international terrorist organizations

2007 Cyberattacks against Estonian institutions

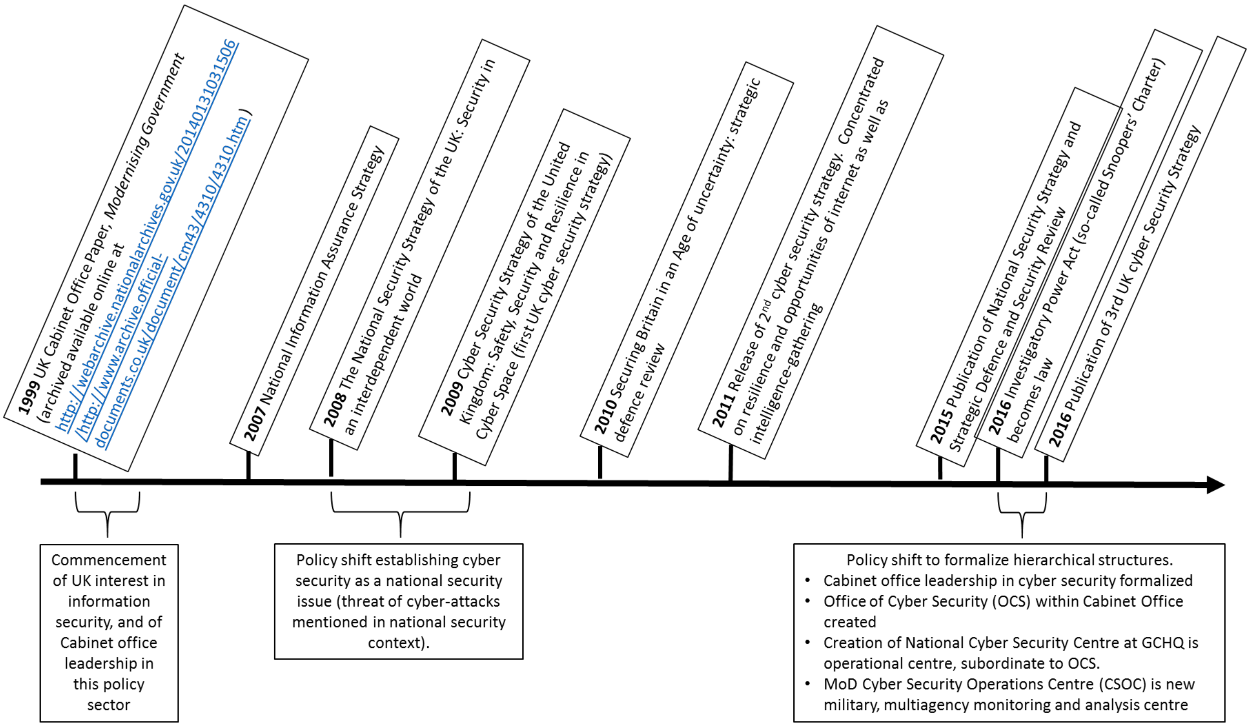
2010 Discovery of Stuxnet

2013 Snowden revealed the large-scale surveillance programme of the US and the UK which has been seen as a threat to state-sovereignty by many states including US and UK allies

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



1999 UK Cabinet Office Paper, *Modernising Government* (archived available online at http://webarchive.nationalarchives.gov.uk/20140131031506/http://www.archive.official-documents.co.uk/document/cm43/4310/4310.htm)

2007 National Information Assurance Strategy

2008 The National Security Strategy of the UK: Security in an interdependent world

2009 Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space (first UK cyber security strategy)

2010 Securing Britain in an Age of uncertainty: strategic defence review

2011 Release of 2nd cyber security strategy. Concentrated on resilience and opportunities of internet as well as intelligence-gathering

2015 Publication of National Security Strategy and Strategic Defence and Security Review

2016 Investigatory Power Act (so-called Snoopers' Charter) becomes law

2016 Publication of 3rd UK cyber Security Strategy

Commencement of UK interest in information security, and of Cabinet office leadership in this policy sector

Policy shift establishing cyber security as a national security issue (threat of cyber-attacks mentioned in national security context).

Policy shift to formalize hierarchical structures.

- Cabinet office leadership in cyber security formalized
- Office of Cyber Security (OCS) within Cabinet Office created
- Creation of National Cyber Security Centre at GCHQ is operational centre, subordinate to OCS.
- MoD Cyber Security Operations Centre (CSOC) is new military, multiagency monitoring and analysis centre

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)[133] 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 cooperation 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[134]

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 sub-section 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. Coordination 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 cyberthreats 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 cyberintelligence 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 cybercriminality. While not made clear, it is implied that UK police handle criminal activity while the military focus on foreign activity. The NCSS provides

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

[134] A 2011 report by the CCDCOE examines the background and current state-of-play (as at 2011) of UK cybersecurity 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 cybersecurity measures. Some info used here

a public face for all cyber-activities, including those of a classified nature (UK Government, 2016, p. 29). The 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 cyberspace (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 cyberdefenses including "offensive cyber capabilities" (UK Government, 2015, p. 41) developed as part of a National Offensive Cyber Programme (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 cooperate 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 cooperation 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. Cooperation 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).[135] 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

[135] 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)

policy. The majority of malicious activity in cyberspace is criminal, and by tackling this aspect other potential malicious cyber-activity – even from a hard, national security perspective – can be reduced.

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 Programme (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 cooperation 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 cooperation 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 Programme (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 sub-section 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[136] - whether the Armed Forces are committed to providing assistance in the event of a cyber-incident 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 cooperation 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

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

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 (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 cyber-incidents 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 Programme 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.

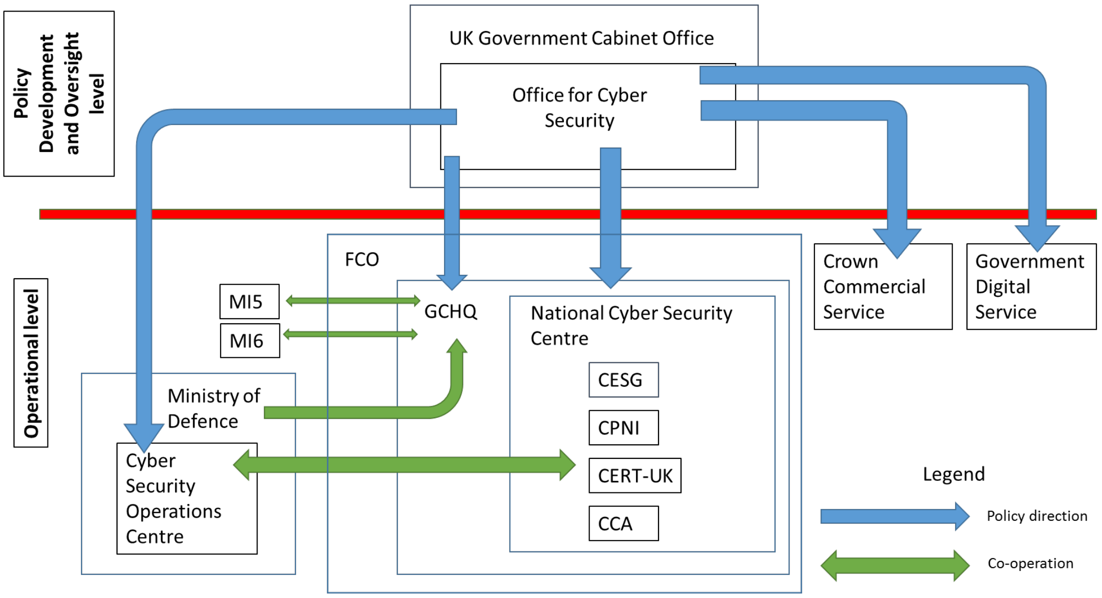
Of note is the fact that operational and cooperative partners listed include BRICS states. These are not traditional security partners for the UK, nor do they share the same long-standing, developed relationships such as those with NATO or the US. In recent years, however, BRICS countries, particularly 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 cooperation.

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


Policy Development and Oversight level
Operational level
UK Government Cabinet Office
Office for Cyber Security
FCO
MI5
MI6
GCHQ
National Cyber Security Centre
CESG
CPNI
CERT-UK
CCA
Ministry of Defence
Cyber Security Operations Centre
Crown Commercial Service
Government Digital Service
Legend
Policy direction
Co-operation

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 cyber-incidents 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 Programme. 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[137]. 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.

[137] 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, cooperation between the public and private sectors is crucial to achieving cybersecurity goals, and only the UK government can take the initiative and drive that cooperation. 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 cyberspace. 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 cyber risks 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 acknowledgment 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 cooperation. 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 cooperation 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 cooperation 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
Cyber-incident	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
Cyber resilience	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 Programme
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 cyberspace.
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[138]*, Sean Cordey*
Center 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 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 second edition builds on the findings of the first, which ranged 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 below.

1. Evidence of a process of transformation

At the general level, the snapshots confirm a process of transformation in policy priorities. Nation states have, over the last decade, systematically formulated 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 ensure 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 solution-building approaches and the 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.

One characteristic of this process is that its evolution has followed a relatively similar trajectory in all cases, strongly influenced by various national and international cyber-incidents. Indeed, from the early 90s until the mid-00s, states were primarily focused on protecting and increasing the resilience of their national and governmental critical (information) infrastructures. Then, the 2007/2008 cyberattacks against Estonian and Georgian institutions raised awareness and led to an increasing politization and securitization of cybersecurity and cyberdefense and its transition from a technical domain to a multidimensional one (e.g. political, economic, social…). For many states, this dynamic was further reinforced in 2010 with the discovery of Stuxnet, which illustrated the interest and capabilities of (powerful) states to conduct cyber-operations. As mentioned earlier, many states responded in the early 10s by conceptualizing the first generation of National Cybersecurity Strategies, which were mainly focused on developing their respective national cybersecurity infrastructures and capacities. At the European level, this tendency was reinforced by the EU's Cybersecurity Strategy and the 2016 Network and Information Security (NIS) directive, which required member states to develop their own cybersecurity strategies. The second generation of cybersecurity strategies – such as those of the Netherlands, France, Germany or Italy – were created in the mid-10s and focused on streamlining, correcting and prioritizing the previous policies, rationalizing the cybersecurity structure (e.g. by including the military forces) and further developing capabilities and general awareness among the population.

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.

[138] Robert S. Dewar is now Head of Cyber Security at the Geneva Centre for Security Policy.

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 apparatuses (such as defense ministries and army commands) to develop strategic responses to cybersecurity threats. Cybersecurity is often approached in a holistic manner, as an overarching framework which includes low-level cybercrime[139] as well as national security implications. Cyberdefense is more commonly applied as a facet of national security. It concentrates on keeping national digital infrastructures secure and ensuring that 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 the development and use of offensive capabilities to respond to cyberattacks in some cases. The Netherlands and Austria are the only states recognizing offensive capabilities openly in their policy documents.

2. Precise policy remains vague

The clarity present in policy development and 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 substitute "digital", "ICT" or "Infocomm" 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 do 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 and contributes to the overall conceptual and definitional haze which continues to surround cybersecurity and cyberdefense. This demonstrates a lack of maturity of definitions. However, through a comparison of the various definitions of "cybersecurity" presented in the different NCSSs and other related policy documents, one can try to alleviate this lack of clarity by identifying core ideational traits common to most if not all national conceptualizations of the terms. Accordingly, three core ideational traits can be found, namely that cybersecurity can be 1) a desired end state or the sum of measures to 2) protect various objects, which range from data to information systems and/or critical infrastructures, 3) against different sets of threats, whether they are technical, organizational, social or natural. Conducting the same exercise on the term "cyberdefense" is, however, more complex, with only five out of the eight states having a dedicated definition for the term. Considering these, the common traits are that cyberdefense comprises of 1) a range of preemptive or reactive state/military technical and non-technical measures (e.g. ICT and information security techniques, computer network operations, intelligence to surveillance) 2) in order to defend/protect cyberspace – or in cyberspace – operational capability and critical systems (e.g. IT and weapons systems).

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 cyberdefense 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 organizational frameworks for policy-making and implementation first, *and then* to develop policy. States establish units or agencies with responsibility for cybersecurity 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 expertise and experience in these fields with the object of identifying, developing and implementing policy solutions. In the case of policy implementation, there is a clear tendency towards establishing specific organs of government and new public bodies to provide information and/or practical assistance in preventing cyber-incidents or providing rapid-response resources in the event of an incident.

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

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 at the strategic level 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. Meanwhile, at the level of operations and day-to-day tasks, the reverse trend can be observed, with five out of eight cases tending towards a decentralized model in which various ministries and bodies are responsible for their own cyber preparedness and the management of cyber-related issues relevant to their statutory tasks.

The second is that, when centralized structures and frameworks of cooperation 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. The only exception to this trend was found in Singapore, where the cybersecurity and cyberdefense agencies are directed and managed by the same former general with strong ties to the military. 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 in 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, at or just below prime ministerial/chancellor level. In most cases it is within the ministry of the interior, with the involvement of the ministry of defense and foreign affairs. There are, however, some exceptions, notably Singapore and Finland, where leadership is held by a dedicated ministry – the Ministry of Communication – while in the Netherlands it is held by the Ministry of Security and Justice. Furthermore, 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 in case of a cyber-incident 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 also 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 cyber-incidents are criminal in nature and therefore have widespread socio-economic effects, such as eroding 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 cyber-incidents, 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 cyber-incident 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 coordination and direction all of the resources of a state, or group of states, towards achieving security (Liddell Hart, 1967). This principle of committing 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 consequently all resources and capabilities available to a state are being committed to achieve cybersecurity. In addition, not only are all of 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 a number of cases, notably France, Singapore, Austria, Italy 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 existing centers of expertise. An example is the centralization undertaken by Germany, Italy and the UK. In all three cases, rather than reinventing the wheel, a center of excellence already operating in a particular policy sector – the BSI in Germany, the DSI in Italy and the UK's GCHQ – is given an expanded remit and tasked with operationalizing that policy. In other cases, such as Singapore with its CSA, this form of centralization takes the form of merging existing poles of expertise into one single agency. 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 from the intelligence services and military, was established to operationalize 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 utilizes 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.

Centralization is, however, not the only approach chosen by states. Indeed, if one compares the cybersecurity architecture of the Netherlands and Austria to the rest of the cases, both are relatively decentralized. The reasons for this are multiple and complex but include, among others, historical path dependencies, federalism or bureaucratic rivalries. As for centralization, decentralization presents both advantages and disadvantages. On the one hand it allows a greater operational flexibility for the different concerned bodies. But on the other hand, decentralization of cybersecurity responsibilities and tasks can lead to greater fragmentation and see the different administrative sectors operate solely within their respective silos, setting their own goals and developing their own approaches according to very different understandings, prioritization and resource allocations.

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

In the main, the countries examined in the collected snapshots have pursued economic and military partnerships with traditional organizations. For European countries, multilateral bodies such as the EU, NATO, the OSCE and OECD were frequently represented. When it comes to non-European states, one can observe a similar gravitation around regional partnerships and bodies, such as ASEAN for Singapore. Meanwhile, bilateral cooperation or consultation is on the rise, mostly through signing Memorandums of Understandings on the pooling and sharing of cyber ranges capabilities. As such, small states such as Austria and Singapore seem to favor this approach, with the former having signed over five MoUs in the last few years and opened bilateral consultation with Russia and Israel. 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 among the majority of 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, France, Italy and the Netherlands are close partners with the EU. This is not to say that these states value their membership of NATO less. Rather, they apply 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 and Austria; two countries which are members of the EU but not of NATO. Although both participate in NATO's Partnership for Peace, they have chosen not to pursue full membership, but nevertheless are close NATO 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 as 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. Indeed, France, Austria and the UK mentioned BRICS and/or 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 (e.g. through NORDEFCO).

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 cybersecurity solutions, particularly given the level of private ownership of Internet and World Wide Web infrastructures. Precise details of public-private partnerships (PPPs), however, are scarce in the policy documents examined. Very little information is provided beyond historical 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. Nonetheless, one can discern some difference in the target sectors of these PPPs. For example, the ones in the Netherlands and Italy are dedicated to cybersecurity in a holistic fashion. Meanwhile, Germany and Austria have adopted critical infrastructure-centric PPPs, while Singapore is focused on fostering its cybersecurity ecosystem through a PPP with and financial support to industries active in cybersecurity.

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 this acknowledges where technical expertise and innovation reside. However, it sets a policy precedent, potentially opening the door for private-sector entities to carry out cyberdefense operations. Responsibility 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 open-source policy documents. Furthermore, it is also interesting to note that in addition to their traditional information sharing, trust building and crisis response responsibilities, some PPPs have also been given increasing national and strategic advisory responsibilities. For example, the Dutch Cyber Security Council is tasked not only with providing guidance to the Dutch Cabinet on the issue of the cybersecurity strategy's and research agenda's implementation development but also with conducting awareness campaigns.

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 and integration of cyberdefense policy and national security. In three cases cyberdefense is a separate policy area (France, Germany and the Netherlands) with their own strategies or policy documentation. In other cases, such as the UK, Finland, Italy, Austria and Singapore**,** cyberdefense is integrated with 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 included cyberdefense in 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.

Further prioritization of cyberdefense as a national security issue can also be observed by examining the (re)configuration of the armed forces. Indeed, in most of the studied cases the cyberdefense bodies are localized at the highest level of command, and in some cases, such as France and the Netherlands, they are directly under aegis of the army's head. In NATO states, such prioritization and centralization is particularly identifiable, as all of the ones examined in this study have created – similar to the American one – their own cyber commands over the past five years. Meanwhile, even non-NATO states such as Finland and Austria are considering developing cyber commands.

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 of each state's intelligence agencies in cybersecurity and cyberdefense. 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. Among these, one notable example is that of the Netherlands, which have, in an effort of centralization, resource and expertise sharing, set up a joint SIGINT cyberunit which reunites its military and civilian intelligence services. 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 increased national scrutiny of the activities of intelligence agencies will produce greater policy transparency in this regard.

9. Conclusion

The examination in this collection of eight important actors has yielded important findings, not least that precise policy and clear definitions in this field remain rare, 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 regarded as evolving 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 such 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 an 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.

Raymond Bierens

Raymond Bierens MSc MC started as an external PhD candidate at the Delft University of Technology and is now connected to the University of Amsterdam for the finalization of his research. His research topic is to investigate the risk models used in cyber strategies to meet with the changing demands of cybersecurity and digitization in both the public and private sectors. Raymond has 19 years of experience with (inter) national organizations in Defense, Security and Vital Infrastructure as Global Vice President at Atos. In addition to his research, Raymond advises start-ups, several Dutch Ministries and (inter)national profit and non-profit organizations in the public and private sectors. As a teacher, he is a frequent lecturer at the Cyber Security Academy, The Hague University of Applied Sciences, VU Amsterdam and the Dutch Government Academy (Rijksacademie). He has published about his research in various journals and magazines such as Springer, GOV Magazine and the National Cyber Security Council magazine**.**

Dr. Matteo E. Bonfanti

Matteo E. Bonfanti is Senior Researcher at the Center for Security Studies. He holds a PhD from the Scuola Superiore Sant'Anna di Pisa. Matteo's research activities focus on the governance implications generated by targeted initiatives adopted by the EU and its Member States to foster their internal security. These include the development and adoption of new technical, technological and organizational solutions to enhance policing and intelligence cooperation, cybersecurity, as well as crisis and emergency management. Before joining the CSS, Matteo was researcher at the Institute of Law, Politics and Sustainability of the Scuola Superiore Sant'Anna, the Centre for Science, Society and Citizenship in Rome, and the Central European University in Budapest. In 2008 he served as research assistant at the office of the European Data Protection Supervisor (EDPS) in Brussels. Matteo has been actively involved as researcher in several EC and EDA funded projects the field of security (counterterrorism, crime prevention, border security, and cybersecurity) since 2010.

Nicolas Castellon

Nicolas is a senior Policy advisor at dcypher with more than 7 years of experience in the technology domain. His main areas of expertise are Cyber Security Governance, ICS/SCADA Security, and Crisis Management. He works on complex projects as a Cyber Security Manager on both the technical and policy levels. He has worked in various sectors, including Dutch government, EU Agencies, Manufacturing, Aerospace, and the Energy sector. He also draws from his experience from the NGO and think tank sectors, having worked at United Nations in New York City, The Hague Centre for Strategic Studies, and the Getulio Vargas Foundation in Rio de Janeiro, where he has co-published various reports on Cyber Security. Nicolas is also a frequent guest lecturer at Utrecht University and Leiden University where he lectures on Cyber Security Governance and Cyber Conflict. Nicolas graduated from Leiden University with a Master of Science (cum laude) in Crisis and Security Management, specializing in Cyber Security Governance of the European Union.

Sean Cordey

Sean is the project assistant of 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 and is pursuing a double degree in international governance, law and diplomacy with the University of St. Gallen and the Fletcher School. His BA thesis was a comparative policy analysis of the cybersecurity strategies of Switzerland, Austria and Germany.

Dr. Robert S. Dewar

Robert Dewar is the Head of Cyber Security at the GCSP in Geneva. 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 cybersecurity policy-making. Robert's research interests cover cybersecurity and defense policy, security studies, the European Union and historical institutionalism. Robert worked as a Senior Researcher at the CSS from 2016 to 2018. 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, cybersecurity and the European Union.

Francis Domingo

Francis Domingo is Assistant Professor and currently the Vice Chair of International Studies Department of De La Salle University. His research focuses on the intersection of networked technologies, foreign policy, and military strategy. His PhD thesis explored the cyber strategy of small states in the Asia-Pacific Region. Before joining academia, he briefly worked with the Office of Strategic and Special Studies (OSS), Armed Forces of the Philippines and RVDBic, a pioneering business risk and intelligence consultancy based in the Makati City, Philippines.

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 cybercriminals.

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.