CSS CYBER DEFENSE

National Cybersecurity Strategies in Comparison – Challenges for Switzerland

Zurich, March 2019

Center for Security Studies (CSS), ETH Zürich

CSS ETH Zurich

ETH zürich

Authors: Marie Baezner, Sean Cordey

Additional research: Matteo Bonfanti, Robert Dewar, Jasper Frei and Fabien Merz
Layout: Miriam Dahinden-Ganzoni

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

This research was ordered by the Federal IT Steering Unit (FITSU)

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

ETH-CSS project- and quality management: Myriam Dunn Cavelty, Deputy Head for Research and Teaching; and Andreas Wenger, Director of the CSS.

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

Please cite as: Baezner, Marie; Cordey, Sean (2019): *National Cybersecurity Strategies in Comparison – Challenges for Switzerland,* March 2019, Center for Security Studies (CSS), ETH Zürich.

Contents

Synopsis

Digital transformation, which is emerging as one of the major challenges of future years, offers not only wide-ranging advantages, but also harbors new risks and engenders new vulnerabilities. A majority of states has begun to address these by developing national strategies under the heading of 'cybersecurity'. Switzerland published its second 'National Strategy for the protection of Switzerland against cyber risks' (NCS), which identifies main challenges, traces responsibilities and outlines future action, in 2018. This study compares the cybersecurity strategies adopted by Germany, Finland, France, Israel, Italy and the Netherlands in order to place the Swiss approach within a broader international context and elicit the most important future challenges through comparison.

It focuses on key strategies, describing main actors and their tasks (in particular the distribution of tasks between civilian and military authorities in the fields of 'security', 'defense' and 'law enforcement'), and identifying the general challenges for organizing national cybersecurity policies.

The cybersecurity strategies examined share a number of common conceptual elements. Six central aspects have in particular been found across all of the states in the study: a holistic approach which encompasses both national security and socioeconomic aspects; links to broader national security strategies; a central focus on developing defensive cyber capabilities; great appreciation of international cooperation; emphasis on the necessity of cooperating with the private sector; and finally the need for greater awareness, education and information.

The most important differences between the examined states lie in where cybersecurity is positioned within the context of government structures, and who bears which responsibilities. This relates to the extent of centralization, the relationship between civilian and military forces, and the tasks of intelligence and law enforcement services. These differences arise predominantly out of the states' distinct political cultures and ways of organizing their political systems.

Given the global nature of cyber threats, comparable states are confronted with comparable challenges when developing, implementing and maintaining their cybersecurity strategies. We have identified eight challenges:

- the (vertical) integration of national cybersecurity with national security and/or an overall strategy for controlling national resources as efficiently as possible;

- the (horizontal) coordination of different bodies tasked with cybersecurity matters, in particular the challenge of finding the right balance between centralization and reliance on existing competences;

- the promotion of international cooperation and the establishment of international norms of conduct in an environment in which geopolitical fault lines have deepened;

- the creation of sound, resilient structures for crisis management, including efficient crisis communications, and the development of a strong ability to respond to serious incidents which takes this communications aspect into account;

- the development of an adequate situation analysis and a precise analysis of threats, both of which must resist exaggerated assessments of cyber threats despite the difficulty of collecting reliable data;

- the building of capacities and the design of future education and training programmes to address shortages of specialist cybersecurity staff;

- the development of a framework for cooperation with the private sector which promotes national security without hampering innovation; and

- the harmonization of laws and efficient strategies for fighting cybercrime..

Switzerland is also exposed to these challenges. If a small, wealthy state such as Switzerland wishes to secure its future in a digital world, it should ensure that it invests adequately in cybersecurity without excessively expanding the reach and role of government. This requires all parts of government to work towards the same overarching goal. At the same time, capacity-building and the design of education and training programmes likely constitute the most productive approach.

Introduction

All over the world, countries endeavor to shape digital transformation processes to obtain optimal benefit from this technologically controlled change for their societies. However, the spread of digital technologies also entails risks. Their technical substructure is insecure due to technical, economic and political factors, and prone to being exploited for criminal or political purposes. Spectacular, criminally motivated cybercrime and the strategic use of cyberspace have become an everyday reality in a world where the number of attractive targets is growing and cybercrime abilities and competences are becoming more and more sophisticated due to high demand.

It is therefore imperative that the challenges of cybersecurity be met if the digital transformation is to be successful. As a result, most states are reviewing their cybersecurity strategies to ensure that they are better prepared for the risks which are emerging in a more and more closely networked and at the same time more and more politicized and militarized environment. The challenges which need to be met are not exclusively technical in nature: Largescale economic and political cyberespionage, strategic interference campaigns and threats to critical infrastructures of national significance are all issues relevant to security policy.

However, the precise role governments and administrations play in cybersecurity must be elicited and carefully defined through a political process. Critical infrastructures are mainly held by private actors. Cyberspace can be viewed as a common good whose dynamics and use are shaped by an entire ecosystem of state and non-state actors. There is no single solution able to resolve all cybersecurity problems – given the numerous risks associated with digital technologies, the definition of responsibilities and the planning of resource allocations are complex, demanding political tasks.

Switzerland published its second 'National Strategy for the protection of Switzerland against cyber risks' (NCS), which identifies the major challenges and responsibilities in this domain, in 2018. This study compares policies, structures and challenges in the cybersecurity domain in six countries in order to validate relevant endeavors and place them in context:[1]

- Finland
- France
- Germany
- Israel
- Italy and
- the Netherlands

This comparison focuses mainly on:

a) the nature and substance of core strategies;

b) the roles and responsibilities of main actors and bodies (law enforcement, military, intelligence services and civilian bodies), and

c) the challenges these states are exposed to in terms of cybersecurity.

This study is mainly based on primary sources, such as publicly available national cybersecurity and cyber defense strategies, and secondary sources such as media articles and scientific research. All of the documents relied on are publicly available. However, it is important to understand the context and goals of these documents, which are subject to certain constraints:

- First, many national cybersecurity strategies in fact provide very little information about states' actual levels of preparedness or relevant activities, in particular as far as national security and defense are concerned. Strategies are, above all, declarations of intent, which set and signal the future direction of the national cybersecurity agenda for a highly diverse internal/domestic and external/international audience. Germany and France have sector-specific implementation plans (i.e. for IT in administration and for the private sector), while the Dutch implementation plan is still being drafted. Israel does not have an implementation plan.

- Second, states mostly do not publish the precise amount of their cybersecurity expenditure. Any public announcements regarding the size of 'cyber forces' etc. should be met with a certain degree of skepticism. The media occasionally publish estimates of national cybersecurity expenditure, but these are generally extrapolated from national security budgets and do not precisely reflect the actual expenditure individual states incur for cybersecurity. The current risk perception is most immediately influenced by the military and (foreign) intelligence services. However, the activities of both of these government services are naturally secretive, rendering it extremely difficult to collect information on expenditure and practices in this domain. Various major projects focusing on monitoring military budgets are also confronted with

1 These countries were selected to ensure that the analysis extends across an adequate number of different political systems in states located geographically close to Switzerland. Israel was added because the country's approach to cybersecurity is frequently noted as interesting. Furthermore, it needed to be ensured that sufficient material was publicly available.

these difficulties and do not publish any information on cybersecurity expenditure (including the Stockholm International Peace Research Institute (SIPRI), the Global Cybersecurity Index of the International Telecommunications Union (ITU) and Jane's Defence Budgets).

- Third, cybersecurity is a cross-sectoral issue. It is therefore not allocated a central budget, but instead distributed across several items. This fragmentation as well as different definitions of cybersecurity make it difficult to evaluate state expenditure in this domain.

This study comprises three sections. The first section compares the development of cybersecurity, the main political principles it is governed by, and the relevant organizational structures in the states studied. The second section describes eight shared challenges, while the third draws conclusions for Switzerland.

Cybersecurity strategies in comparison

This study compares policies, structures and challenges in the cybersecurity domain in Finland, France, Germany, Israel, Italy and the Netherlands. Its core parameters are summarized in the following table:

	Finland	**France**	**Germany**	**Italy**	**Israel**	**Netherlands**
Year of first published strategy	2013	2011	2011	2013	2011	2012
Year of current strategy	2013	2015	2016	2017 (National Plan)	2015	2018
Separate defense strategy	No	Yes	No	No, but the military is covered by the 2017 National Plan	No	Yes
Definition of cybersecurity	Yes	Yes (in the 2011 NCSS)	Yes	No	Yes	Yes
Lead agency/body	UTVA and security committee (civilian)	Prime Minister (civilian)	Minister of the Interior (civilian)	President of the Council of Ministers (civilian)	Prime Minister (civilian)	Minister of Justice and Security (civilian)
Organizational structure	Centralized at the strategic, decentralized at the operational level	Centralized	Decentralized	Mixture of centralized and decentralized	Centralized	Decentralized
Defensive cyber capabilities	Yes	Yes	Yes	Yes	Yes	Yes
(explicitly referred to in the strategy)	No	No	No	No	No	Yes
International cooperation	Yes	Yes	Yes	Yes	Yes	Yes
Cooperation with the EU	Yes	Yes	Yes	Yes	No	Yes
Cooperation with NATO	Yes	Yes	Yes	Yes	No	Yes
Cooperation with the OSCE	Yes	Yes	Yes	Yes	No	Yes
Cooperation with the private sector	Yes	Yes	Yes	Yes	Yes	Yes
Awareness-raising/ education/information regarding cybersecurity	Yes	Yes	Yes	Yes	Yes	Yes

Each state has its own political history, institutions, and political decision-making processes, and significant operational differences therefore arise between them as they engage with new political issues such as cybersecurity. It is, however, evident that there is also a large number of conceptual similarities between these states. The following section identifies both similarities and differences between the analyzed states in order to provide a better understanding of national cybersecurity strategies and the challenges these states share in this domain.

Core documents and their development

All six states have developed national cybersecurity strategies over the past ten years. This development underlines both their increasing awareness of cyber threats and their determination to better protect their networks and infrastructures against them. Their current strategies have evolved as part of a broader development that has been strongly influenced by specific incidents in cyberspace with international implications.[2]

From the early 1990s until the mid-2000s, cybersecurity policy focused on protecting critical infrastructures and state networks against cyberattacks. Cyberattacks against Estonian institutions in 2007, and the war between Russia and Georgia in 2008, which involved both ground combat and disruptions of enemy cyberspace, illustrated that cybersecurity could no longer be limited to purely technical aspects.

As a result of these events, states began to broaden their understanding of cybersecurity to include both the technical and the political domain. In 2010, the world discovered Stuxnet, malicious software designed to damage centrifuges in an Iranian nuclear facility. This incident not only put a spotlight on states' interest in conducting cyber operations and their relevant capabilities, but also accelerated the development of national cybersecurity strategies.

Since 2013, these strategies have focused more and more strongly on building capabilities. Also, the European Union's 2013 cybersecurity strategy and the 2016 EU Network and Information Security directive require member states to develop national cybersecurity strategies.

Six common elements have emerged from relevant efforts:

- First, states have adopted a holistic approach to cybersecurity, which comprises technical capabilities as well as education, information and awareness-raising.

- Second, cybersecurity strategies are aligned and/or integrated with broader national security strategies.

- Third, strategies focus strongly on the need for states to develop defensive cyber capabilities. Only one of the analyzed states (the Netherlands [3]) explicitly discloses that it is developing offensive capabilities to enable it to counter cyberattacks. Naturally, this does not mean that other states are not also intending to develop such capabilities or have already developed them.

- Fourth, all strategies emphasize the significance of international cooperation within the framework of regional and international organizations in order to improve collaboration in the cybersecurity domain. All states except Israel are members of the European Union (EU), and all except Finland and Israel are NATO members. As a result, all states except Israel identify NATO as their main international cooperation partner in the cybersecurity domain. This also includes Finland, which cooperates with NATO through its membership in the Partnership for Peace. Furthermore, all of the states (except the Netherlands) also expressly refer to the OSCE in their strategies, while only the French, Finnish and Dutch strategies make explicit mention of the UN.

- Fifth, all strategies highlight the need for cooperating with the private sector (as numerous critical infrastructures and information assets are privately held). The Netherlands and Italy have adopted an approach involving a special public-private partnership for cybersecurity, while Germany has a public-private partnership with the operators of critical infrastructures only, and the remaining states analyzed in this study prefer to provide funding to industries involved in cybersecurity.

- Sixth, all states emphasize the importance of raising awareness of cybersecurity issues at all levels of society, and the need for better education and information.

However, there are also a number of significant differences in addition to these broad similarities:

- Finland and Italy have not developed separate strategies for their defense ministries and armed forces, but instead include their roles and objectives under their general national cybersecurity strategies. This integration of the armed forces into their cybersecurity strategies is most likely due to political and historic path dependencies, in particular both states' traditionally collaborative, holistic and consensual making of security policy.

- France has published separate strategies for its Ministry of the Interior[4] and Ministry of Defense[5],

2 Kadri Kaska, *National Cyber Security Organisation: The Netherlands* (Talinn: CCDCOE, 2015), https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_NETHERLANDS_032015_0.pdf

3 Ministry of Justice and Security, *National Cyber Security Agenda: A cyber secure Netherlands* (The Hague: Ministry of Justice and Security, April 2018), p. 23, https://www.ncsc.nl/english/current-topics/national-cyber-security-agenda.html

4 Ministry of the Interior, *Stratégie de lutte contre les cybermenaces* (Paris: Ministry of the Interior, 2017) https://www.interieur.gouv.fr/content/download/101310/797848/file/Lutte-contre-les-cybermenaces.pdf

5 Ministry of Defense, *Pacte Cyber Défense* (Paris: Ministry of Defense, February 2014) *http://www.defense.gouv.fr/content/download/237708/2704474/file/Pacte%20D%C3%A9fense%20Cyber-1.pdf*

both of which define clear objectives for these ministries. These additional strategies probably evolved in view of the ministries' specific tasks, the desire to delineate their roles in cybersecurity more precisely, and the aim to signal their different orientations to their business partners, other ministries and international partners.[6]

- While some states update older cybersecurity strategies with new ones, Italy has used its 2013 national strategic framework for cybersecurity[7] as a central strategic document, which is realigned by means of national plans[8] as required. This affords greater flexibility in terms of policymaking.

- The Netherlands have already published their third national cybersecurity strategy and developed a number of complementary cybersecurity strategies on specific issues, in particular the 2017 International Cyber Strategy[9] and the 2015 Cyber Strategy for Defense[10] (second Dutch strategy). The fact that there are different strategies in this domain is due to internal political debates and the desire of the relevant ministries to stake out their respective competencies.

- France stands out from the other states in terms of the terminology used, as its 2015 strategy refers to the concept of 'digital security'[11], which is broader than 'cybersecurity' and also includes online propaganda and disinformation campaigns. This change was made in view of the 2015 terror attacks and increasing Islamic State propaganda in social media.

Roles and Responsibilities

Generally, political and strategic leadership regarding cybersecurity falls within the domain of the most senior political levels. In most of the states studied, national cybersecurity strategies are published by the office of the prime minister, except in Germany and the Netherlands, where the Ministry of the Interior and Ministry of Justice and Security respectively are responsible for the strategy.

The fact that cybersecurity is located at the most senior political levels underlines both the importance of this issue and the fact that it is subjected to civilian leadership. Civilian leadership indicates that governments do not regard cybersecurity as a narrowly defined question of national security or (even more narrowly) as a military issue, but instead as a socioeconomic concern which affects the whole of society.

In most states, the ministries of the interior and defense are also institutionally involved in cybersecurity in addition to the prime ministers' offices. In the Netherlands, the Ministry of Justice and Security takes the lead role in cybersecurity matters, but the Ministry of the Interior, Ministry of Defense and Foreign Ministry are also involved.[12] In Finland, the Ministry of Transport and Communications is responsible for cybersecurity, again with the involvement of the Ministry of the Interior, Ministry of Defense and Foreign Ministry. In the (defensive) prevention of cyber risks, civilian bodies with responsibility for defending the general public share leadership with the armed forces, which are responsible for defending their own infrastructures.

Varying degrees of centralization were found in the states analyzed for this study:

- France is highly centralized, with the National Cybersecurity Agency (Agence nationale de la sécurité des systèmes d'information (ANSSI)) being the most important organization in the domain. However, French law enforcement structures are more strongly fragmented, as this domain is covered by various actors whose tasks include the fight against cybercrime, among others.

- While Finland has centralized cybersecurity at the strategic level, with relevant responsibility being borne by the President and Committee of Ministers for Foreign and Security Policy (UTVA), there is a greater degree of fragmentation at the operational level.

6 Jean-Yves Le Drian, *Présentation du Pacte Cyber Défense* (Paris: Ministry of Defense, February 2014) *https://www.defense.gouv.fr/english/actualites/articles/presentation-du-pacte-defense-cyber*

7 President of the Council of Ministers, *National Cybersecurity Framework* (Rome: President of the Council of Ministers, December 2013) *https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf*

8 President of the Council of Ministers, *National Plan for Protection in Cyberspace and ICT Security* (Rome: President of the Council of Ministers, December 2013) *https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf*; President of the Council of Ministers, *Piano nazionale per la protezione cibernetica e la sicurezza informatica* (Rome: President of the Council of Ministers, March 2017) *https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf*

9 Foreign Ministry, *'Building Digital Bridges' International Cyber Strategy – Towards an integrated international cyber policy* (The Hague: Foreign Ministry, February 2017), *https://www.government.nl/binaries/government/documents/parliamentary-documents/2017/02/12/international-cyber-strategy/International+Cyber+Strategy.pdf*

10 Ministry of Defense, *The Defence Cyber Strategy* (The Hague: Ministry of Defense, February 2015), *https://english.defensie.nl/topics/cyber-security/defence-cyber-strategy*

11 Prime Minister, *Stratégie Nationale Pour la Sécurité Du Numérique* (Paris: Prime Minister, October 2015), *https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/*

12 Ministry of Justice and Security, *National Cyber Security Agenda: A cyber secure Netherlands* (The Hague: Ministry of Justice and Security, April 2018), *https://www.ncsc.nl/english/current-topics/national-cyber-security-agenda.html*

- Israel has had the greatest degree of institutional centralization of defensive cybersecurity aspects since it established its cyber directorate in 2018.

- Italy's institutional structure involves a mixture of centralization and decentralization: It is centralized in that the President of the Council of Ministers bears primary political responsibility in questions of cybersecurity. However, the structures below this level are decentralized, as various bodies share responsibility for cybersecurity and contribute to the country's cybersecurity strategy in interaction with each other.

- German and the Netherlands have decentralized structures. In Germany, decentralization is due to the country's federal political system.

Relationships between the civilian and military domains

In most countries, the civilian and military domains of cybersecurity are separated, with each domain having its own institutions, strategies, tasks and personnel. The armed forces are generally responsible for protecting their own infrastructures, and building offensive and defensive capacities.

In some cases, there is explicit mention of cooperation between civilian and military bodies:

- In France, there is cooperation within the framework of the Operational Center for the Security of Information Systems (Centre d'opération pour la sécurité des systèmes d'information (COSSI)) of the ANSSI and the Analysis Center for Defensive Cyber Operations (Centre d'analyse en lutte informatique defensive (CALID)) of the armed forces. The cooperation between these two institutions also entails the exchange of information, and CALID supports COSSI in the event of a cyberattack on defense companies. The headquarters of COSSI and CALID are located in the same building in order to facilitate collaboration.[13]

- In the Netherlands, cooperation takes place at the level of the Joint SIGINT Cyber Unit (JSCU), which comprises the domestic and foreign intelligence service (AIVD) as well as the military intelligence service (MIVD). Both AIVD and MIVD have separate budgets, separate hierarchies and separate personnel, but work from the same building, share intelligence about incidents and also collaborate in some instances as required.[14]

- In Finland, cooperation takes place at a more senior level via the security committee (TK), which is chaired by the Ministry of Defense, and the Government Situation Center (GOVSITCEN), which is located within the office of the Prime Minister. The armed forces and civilian bodies use the TK to exchange information about planning and developing national security strategies, and the GOVSITCEN to exchange information about threats in order to promote comprehensive, situation-based awareness of cybersecurity issues.[15]

- In Israel, the Cyber Directorate, which reports directly to the office of the Prime Minister, is responsible for the exchange of information.

There is also some cooperation between the armed forces and the private sector. This type of cooperation is mainly found between the armed forces and private actors responsible for managing critical infrastructures in order to protect such infrastructures against cyberattacks.

Cybersecurity in the armed forces

Cybersecurity is organized similarly in the armed forces of all six analyzed states. Each state has a cybersecurity body at the most senior command level, often immediately subordinate to the commander-in-chief of the armed forces. This constellation shows that the states are aware of how important cybersecurity issues are for all parts of the armed forces.

This prioritization and centralization of cybersecurity within the military is particularly evident among NATO members. All of the NATO members analyzed in the study established cyber commands between 2014 and 2017. It is unclear whether the stimulus for creating cyber commands emanated from NATO or NATO members, but these bodies constitute a clear, general trend among NATO members. The cyber commands work towards centralizing and monitoring defensive cyber activities of the armed forces. Finland is not a NATO member and has not yet established a cyber command but considers the creation of such a body. Israel had planned to establish a

13 Ministry of Defense, *Pacte Cyber Défense* (Paris: Ministry of Defense, February 2014) *http://www.defense.gouv.fr/content/download/237708/2704474/file/Pacte%20D%C3%A9fense%20Cyber-1.pdf*; Pascal Brangetto, National Cyber Security Organisation: *France* (Talinn: CCDCOE, 2015), S. 12, *https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_FRANCE_032015_0.pdf*

14 Kadri Kaska, *National Cyber Security Organisation: The Netherlands* (Talinn: CCDCOE, 2015), p. 17, *https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_NETHERLANDS_032015_0.pdf*

15 Cf. Sean Cordey, Finland', in *National Cybersecurity and Cyberdefense policy snapshots,* (Zurich, Center for Security Studies, September 2018), *http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports_National_Cybersecurity_and_Cyberdefense_Policy_Snapshots_Collection_1.pdf*

central cyber command, but ultimately decided to maintain its separation between defensive military capacities (directorate C4I) on the one hand, and signals intelligence and the conduct of cyberattacks (unit 8200 of the Military Intelligence Directorate) on the other.[16]

All armed forces have their official military IT emergency response teams (Computer Emergency Response Teams/CERTs), which protect their respective networks. Italy has a central CERT for its entire armed forces, which is assisted by additional CERTs for individual parts of the military.

The role of intelligence services

The role of intelligence services is not often explicitly stated in national cybersecurity strategies due to the sensitive, secret nature of their activities. If intelligence services are mentioned in strategy documents, this is usually done in order to position them within the broader national cybersecurity framework. To the extent that their role is described, this is done in the context of counterespionage and situational awareness of cyber threats. Intelligence services are frequently under civilian control and therefore report to the most senior political levels, for example the Prime Minister, Chancellor, or Minister of defense or the interior.

In this context, three countryspecific particularities are of note:

- In France, the Directorate-General of Internal Security (Direction Générale de la Sécurité Intérieure (DGSI)) depends on the Directorate-General of External Security (Direction Générale de la Sécurité Extérieure (DGSE)) in terms of surveillance structures. However, DGSI is building its own infrastructures to achieve independence.[17]

- In Israel, the intelligence services (i.e. Aman for the military, Mossad for foreign intelligence, and Shin Beth for domestic intelligence) likely have offensive cyber capabilities.

- In Italy, the Security Information Department (Dipartimento delle Informazioni per la Sicurezza (DIS)) gathers and coordinates cybersecurity information from the foreign intelligence service (Agenzia Informazioni e Sicurezza Esterna (AISE)) and domestic intelligence service (Agenzia Informazioni e Sicurezza Interna (AISI)).

Law enforcement

Law enforcement authorities are involved in cybersecurity issues, as they investigate and fight cybercrime and cyberenabled crime. In all of the states examined for this study, the tasks and structures of law enforcement authorities are separated from those of other institutions concerned with cybersecurity and, above all, from military institutions, as one might expect of democratic countries.[18] Their specific tasks lie in examining and investigating illegal internet contents, cyberenabled crime and cybercrime, as well as in raising awareness of these threats and assessing associated risks. All countries provide for separation between bodies responsible for identifying and monitoring illegal internet contents, and those responsible for fighting cybercrime. Furthermore, Germany, for example, includes units specializing in combating organized crime in cybercrime investigations. European states cooperate in cybercrime matters via EUROPOL at the European level, and all states cooperate internationally via Interpol.

There are three notable observations regarding particularities in individual states:

- In France and Italy, law enforcement is fragmented. This is due to existing structures which were assigned additional responsibilities in fighting cybercrime and cyberenabled crime.

- Italy has a special unit, the National Anti-Crime Computer Center for Critical Infrastructure (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC)), which fights cybercrime aimed against critical infrastructures.

- The German and Dutch law enforcement authorities have developed cooperation platforms with the private sector. In Germany, the Central Cybercrime Unit (Zentrale Ansprechstelle Cybercrime (ZAC)) acts as a point of contact for companies exposed to criminal cyberattacks. In the Netherlands, the law enforcement authorities established the Electronic Crimes Task Force as a public-private partnership with the private sector.

16 Judah Ari Gross, *Army beefs up cyber-defense unit as it gives up idea of unified cyber command* (Jerusalem: The Times of Israel, Mai 2017), https://www.timesofisrael.com/army-beefs-up-cyber-defense-unit-as-it-gives-up-idea-of-unified-cyber-command/

17 Jacques Follorou, *Pris dans leurs rivalités, les services français ont privilégié leurs liens avec la NSA et le GCHQ* (Paris: Le Monde, December 2016), https://www.lemonde.fr/pixels/article/2016/12/10/pris-dans-leurs-rivalites-les-services-francais-ont-privilegie-leurs-liens-avec-la-nsa-et-le-gchq_5046755_4408996.html

18 Italy forms an exception in that the *carabinieri* are a military force exercising police tasks.

Main challenges

As most of the states examined for this study share a similar threat environment, all of their governments are confronted with a number of challenges in terms of developing, implementing and maintaining comprehensive, holistic cybersecurity strategies.

We have identified eight main challenges:

1. the (vertical) integration of national cybersecurity strategies with national security and/or overall strategy frameworks;
2. the (horizontal) coordination of the various bodies involved in cybersecurity;
3. international cooperation and norm-setting;
4. crisis management;
5. situation analysis and analysis of cyber threats;
6. capacity-building, education, information and awareness-raising;
7. the creation of a functional cooperation framework with the private sector; and
8. the harmonization of legislation.

1. Integration (vertical)

States are struggling to integrate national/international cybersecurity visions and goals into their broader national security frameworks. One of the difficulties faced is the conceptual transition from regarding cybersecurity as a technical problem to viewing it as a political challenge. Cybersecurity is a cross-sectoral issue which overlaps with many other political domains, some of which have longer traditions, among them information security, the protection of critical infrastructures and general defense. These domains have been shaped by numerous established strategies, laws, regulations and political processes. The challenge now is to coordinate and integrate all existing policies, which are frequently isolated from each other, in order to create a cohesive, networked, streamlined framework or overall strategy. Conceiving of and treating cybersecurity as a separate issue and failing to integrate it with existing policies must be avoided.

2. Coordination (horizontal)

The second challenge relates to the definition and efficient implementation of policies and measures. Difficulties arise from the heterogeneity of the actors involved in cybersecurity and cyber defense at the vertical (national, regional, local) and horizontal (civilian and military, public and private) levels. The aspects to be coordinated include the institutionalization of collaboration between public bodies; the necessary transformation of certain, often deeply ingrained bureaucratic habits and routines; the mainstreaming of relevant dialogue and terminology among all actors involved; the harmonization of the different operational logics of the private (for-profit) and public (not-for-profit) sectors; and the development of new technological knowledge and capacities with limited resources and experiences. Coordinating the various actors' divergent interests and positions can require large amounts of time, energy and resources and be characterized by rivalries. This is often the case where resources need to be allocated or reallocated, which frequently results in bureaucratic wrangling about budgets and competencies (for example in Israel[19]). Furthermore, complex bureaucratic responsibilities and monitoring structures (for example among the bodies responsible for cybercrime in France and Italy) can make it virtually impossible to implement efficient overarching controls.

3. International cooperation

A third challenge concerns international cooperation in the context of decentralized, fragmented governance structures for cybersecurity (and the internet in general), and compliance with norms for good or responsible conduct in cyberspace. The former has caused a multiplication of processes, which has resulted in cyber diplomacy requiring greater (personnel, economic and political) resources and gaining greater importance. This is particularly problematic for states with a limited diplomatic corps (for example Finland). At the same time, current geopolitical tensions render dialogue, trust-building, cooperation and crisis prevention difficult. Foremost, however, there is a widening gap between the international community's collective desire for greater stability and some states' actual, offensive practices, as states continue to jostle for influence in cyberspace.

19 Lior Tabansky & Isaac Ben Israel, *Cybersecurity in Israel* (New York: Springer Briefs in Cybersecurity, 2015), https://www.springer.com/de/book/9783319189857

4. Crisis management

The fourth challenge concerns three interrelated issues: maintaining efficient crisis communication, building clear structures for crisis communication, and developing adequate capacities for responding to incidents. In the event of a major cyber crisis, the efficient, continuous flow of information between the responsible public and private bodies is decisive if an appropriate response is to be found and implemented, but this can be difficult if there are no institutionalized channels for exchanging information. Furthermore, public communication can be problematic and sensitive for both the public and the private sector and even be counterproductive, unless it is organized appropriately. A fundamental difficulty in this regard is to offer the right incentives to the private sector to ensure that government bodies are notified, support is requested, and cooperation is implemented in case of incidents. The absence of clearly defined, proven leadership structures can further hamper governments' ability to respond. At the same time, whole-of-government contingency plans and response exercises are extremely complex (and expensive) to prepare and conduct, given the cross-sectoral nature of the issue and the large number of actors involved. Finally, it is difficult to build and maintain sufficient numbers of appropriately qualified personnel that is available at call and able to respond adequately to incidents.

5. Situation analysis

The fifth challenge consists in building and maintaining a consistent situation analysis which is both holistic and focused on detail and involves a careful assessment of risks, while also securing efficient, effectively coordinated flows of information between all (civilian and military) actors who gather and aggregate data, including intelligence services, national cybersecurity centers and the armed forces, among others. In this context, there has long been the risk of overstating cyber threats and attaching too much weight to worst-case scenarios. If there is no shared view of the threat situation among the different services which gather cybersecurity information, this constitutes another risk that needs to be considered. Also – without intending to trivialize the challenges of digitalization – disproportionate risk assessments do not provide a sound basis for developing solutions. The issue of balancing freedoms (such as privacy rights) with security is of decisive significance in all democracies. Independent analytical capabilities, which facilitate the identification of risks in the national context, thus allowing them to be addressed, are crucial for this purpose.

6. Education, information and capacity-building

Another challenge consists in building capacities and providing for relevant education and information. This problem is becoming ever more urgent, as there is a serious shortage of qualified employees in the cybersecurity domain even now (about 142,000 within the EMEA region and 2.93 million worldwide[20]), which is likely to become significantly worse. This shortage concerns not only cybersecurity specialists, but also generalists, technical specialists, political decision-makers and academics, who all contribute to the seamless function of the private and public sectors. Furthermore, there is the challenge of recruiting and retaining young talents, above all in the public sector, which is perceived to be less attractive than the private sector (in terms of financial rewards and career prospects). In the long term, other political issues may also need to be considered in this context, for example the persistent challenge of building, coordinating and monitoring a holistic, participative national framework for capacity-building initiatives; efforts to ensure that education and training keep up with rapid change in cybersecurity and its operational environment; the ongoing training of public-service employees in how to engage securely with cyberspace, potentially including the further development of existing certifications; and finally the establishment of new, non-conventional qualifications such as digital badges. This latter challenge also relates to the problem of raising awareness, not only within public administrations, but also more broadly in the private sector (for example among CEOs or SMEs), among political elites (i.e. parliamentarians) and the general public. Many states are struggling to identify gaps, define goals and develop mechanisms for creating a culture of data protection, data security and cybersecurity.

7. Public-private partnerships

The majority of critical infrastructures is in private hands, making the issue of public-private partnerships crucial for political decision-making processes in the cybersecurity domain. Governments strive to define appropriate frameworks for relevant cooperations and establish a balance between a prescriptive, government-oriented and cooperative, market-oriented approach. However, public-private partnerships have become the cornerstones of most national cybersecurity strategies and serve as central platforms for meeting both conventional and non-conventional security threats in cooperation with the

20 ISC2, *Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens* (2018), https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx

private sector. Yet many challenges persist[21], among them ongoing ambiguity regarding the details of such partnerships; the general difficulty to define norms; a lack of incentives for the private sector to engage with national security issues; and the problem of expanding the cost-benefit paradigm applied by private actors to build a broader framework designed to promote the public interest. All of this results in a lack of clarity regarding responsibilities, ownership and authority.

8. Legislation and regulation

Finally, there are a number of legal challenges, above all the identification of legislative gaps; the harmonization of laws and jurisdictions with regard to cyberspace and cyber activities; the regulation of the private sector; the issue of encryption vs. law enforcement; and the dynamic change of the technical environment. Moreover, measuring success remains a complex process, as in all contexts of maintaining and controlling public order.

21 Madeline Carr, *Public–private partnerships in national cyber-security strategies* (London: Royal Institute of International Affairs, 2016), *https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf*

Conclusion and challenges for Switzerland

The two strategies for protecting Switzerland against cyber risks (NCS 2012 and 2018) are largely consistent with the six strategies compared for the purposes of this study. Risks are assessed similarly, and the same issues and measures are identified as being particularly urgent. Switzerland is consequently exposed to the same eight risks, albeit to a different extent:

1. Integration: The NCS reflects a holistic perspective of cybersecurity, which is also expressed in the 'National Strategy for the Protection of Critical Infrastructures' (SKI) and the 'Digital Switzerland' strategy. There is, however, no integration with an overarching strategy, although the federal reports on foreign and security policy could serve as strategic guideposts. Yet, a strategic vision for technological issues is essential if Switzerland is to position itself effectively in a world which is undergoing rapid change and digitalization.

2. Coordination: The NCS takes the various bureaucratic units into account together with their roles and responsibilities. Additionally, a cybersecurity center of excellence is being established, which will be headed by a cybersecurity delegate. This new structure is to address the challenge of coordinating different actors, including those outside of government. However, the risk of less-than-optimal solutions and bureaucratic wrangling for competences remains, and new structures still need to prove effective. Moreover, cybersecurity is not an isolated issue, but must be appropriately embedded in a number of different policy domains. Creating parallel structures for cyber issues alone may therefore not lead to the desired success.

3. International cooperation: Switzerland engages actively with the major international efforts to establish cybersecurity norms. However, it could intensify relevant activities, and the position of Geneva as a center of engagement with cybersecurity issues could be strengthened further, keeping in mind that this space is not without competition. Other states also allocate substantial (financial and diplomatic) resources to positioning themselves successfully in the norm-setting process. Another consideration in this context would be to expand the training of the diplomatic corps in cybersecurity issues.

4. Crisis management: Good crisis management and in particular good crisis communication capabilities remain an important political challenge with regard to major cyber incidents. While cyber aspects have been integrated into the processes of established crisis management bodies (such as the Federal Civil Protection Crisis Management Board (BSTB)), experience has shown that dealing with cyber incidents remains a significant political challenge, as knowledge about perpetrators is often limited and the damage caused is difficult to assess. Exercises involving several areas of responsibility are crucial in this context. As it must be expected that most cyber incidents of national relevance will include a political dimension, it is paramount that cybersecurity is viewed as a political as well as technical responsibility.

5. Situation analysis: The availability of good cyber forensic capabilities is just as decisive for states as their ability to integrate several sources of intelligence to develop a holistic perspective. Switzerland tends to assess risks prudently, but the assessment of risks constitutes an ongoing challenge, as the intentions of foreign actors and the dynamics of technological development entail a large number of uncertainties.

6. Education: For states wishing to enter their digital future well-prepared, the most important challenge is probably continued investment in broad research, education, information and innovation. A holistic approach means that cybersecurity is not viewed as a narrowly defined computer science problem, but instead framed as a much more comprehensive social, political and economic issue (as is suggested to some extent in the 'Digital Switzerland' strategy and in the Federal Council Dispatch on the Promotion of Education, Research and Innovation). This allows cybersecurity to be understood as a prerequisite for optimally utilizing the benefits afforded by digitalization, that is as an opportunity for the long-term transformation of the Swiss economy.

7. Public-private partnerships: Switzerland has a proven approach to public-private partnerships in the cybersecurity domain, which is largely based on voluntary participation, though. In the future, it will be important to engage with other models as well, including regulatory measures such as notification obligations, to create financial incentives in certain areas, and to have government take responsibility in case of specific incidents. The challenge will be to design these models such that well-functioning public-private partnerships are not placed at risk.

8. Legislation: Technological challenges are subject to rapid change, which poses difficulties for legislators. Cyber criminals are innovative, and legal systems are

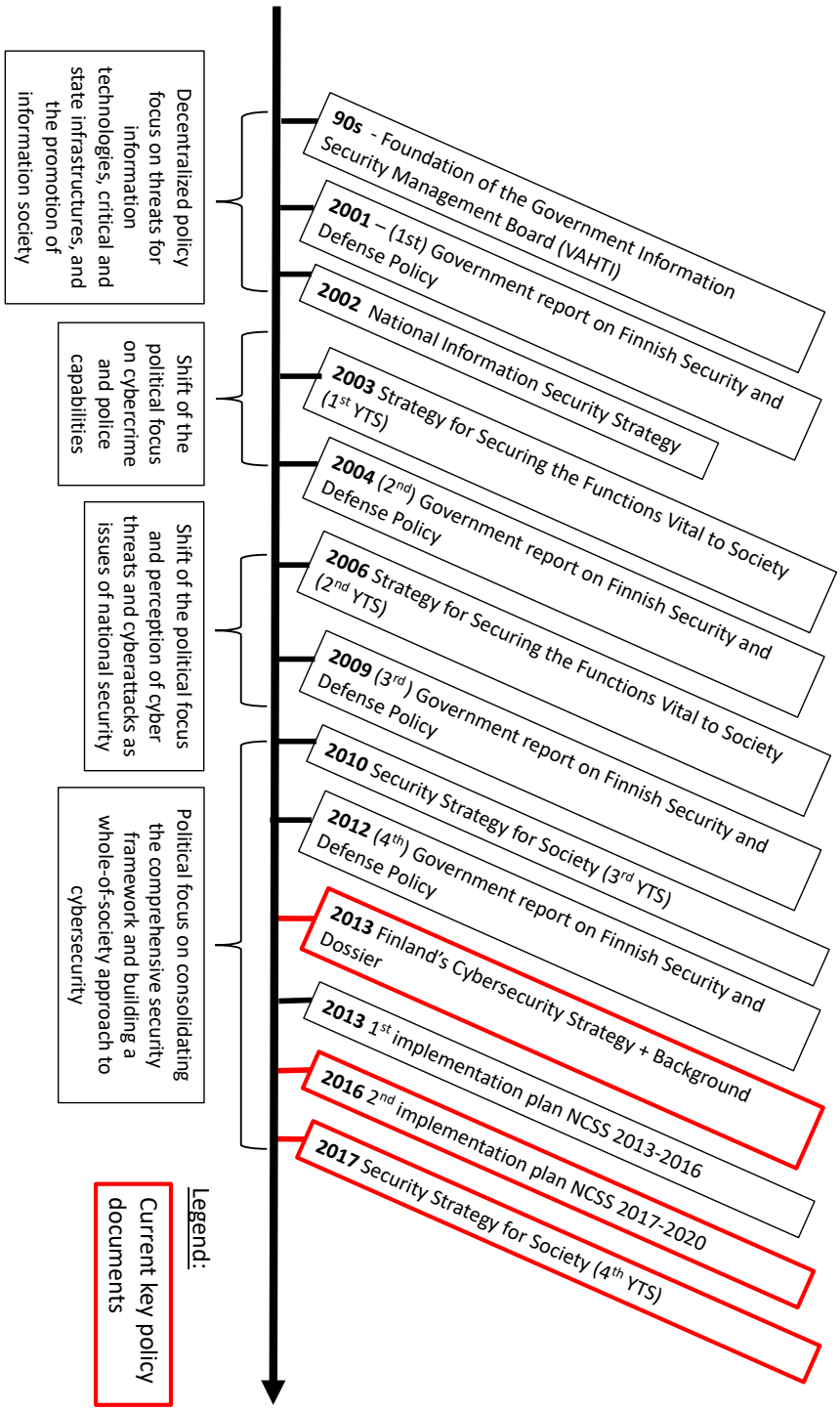
sometimes struggling to keep up with them. It is therefore not only necessary to ensure that law enforcement authorities have good cyber forensic and analytical capabilities but also to exchange information, for example between cantonal police authorities.

As already mentioned above, the size of other states' cyber budgets is unclear. However, given their wideranging activities, it is likely that they are taking the issue seriously, mainly because a development as positive as digitalization depends on state actors' ability to create a certain degree of cybersecurity within their respective societies, i.e. to promote an environment which allows and supports greater cybersecurity. Furthermore, political actors are generally more willing to spend money the more issues are taken seriously. However, Switzerland has to date not (yet) allocated major expenditure to this domain. Most beneficial would be investments in building capabilities, education, research and information, as these produce long-term benefits for all. It must additionally be ensured that the various bureaucratic bodies are aware of what they need to do, and work towards a shared, overarching goal.

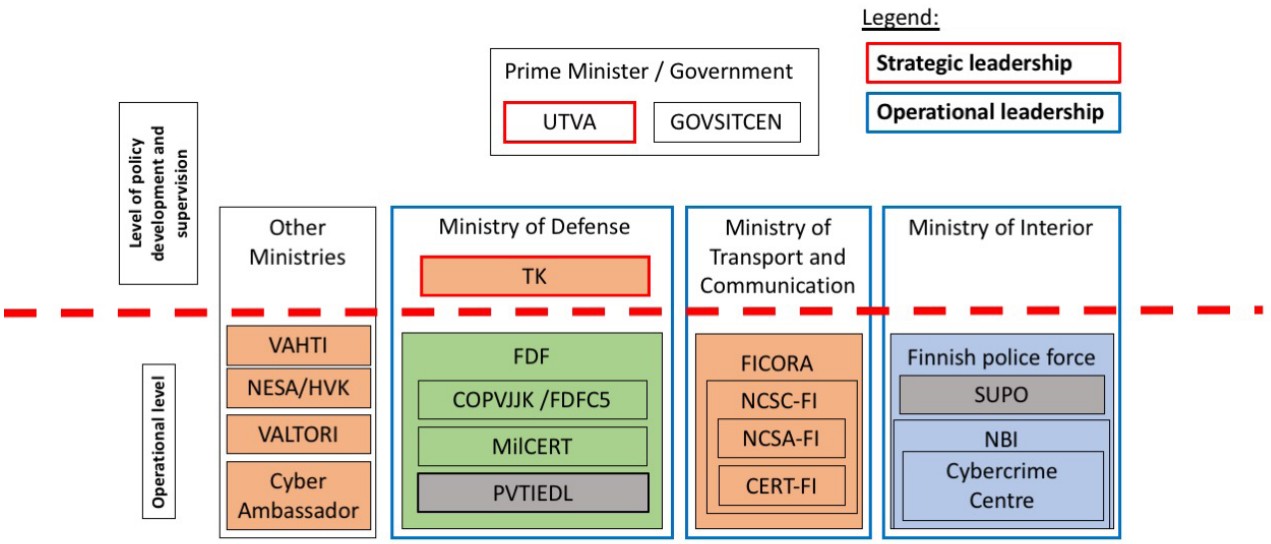
Annex

Country information Finland

1. Core strategy documents and developments



2. Organization, main bodies and responsibilities



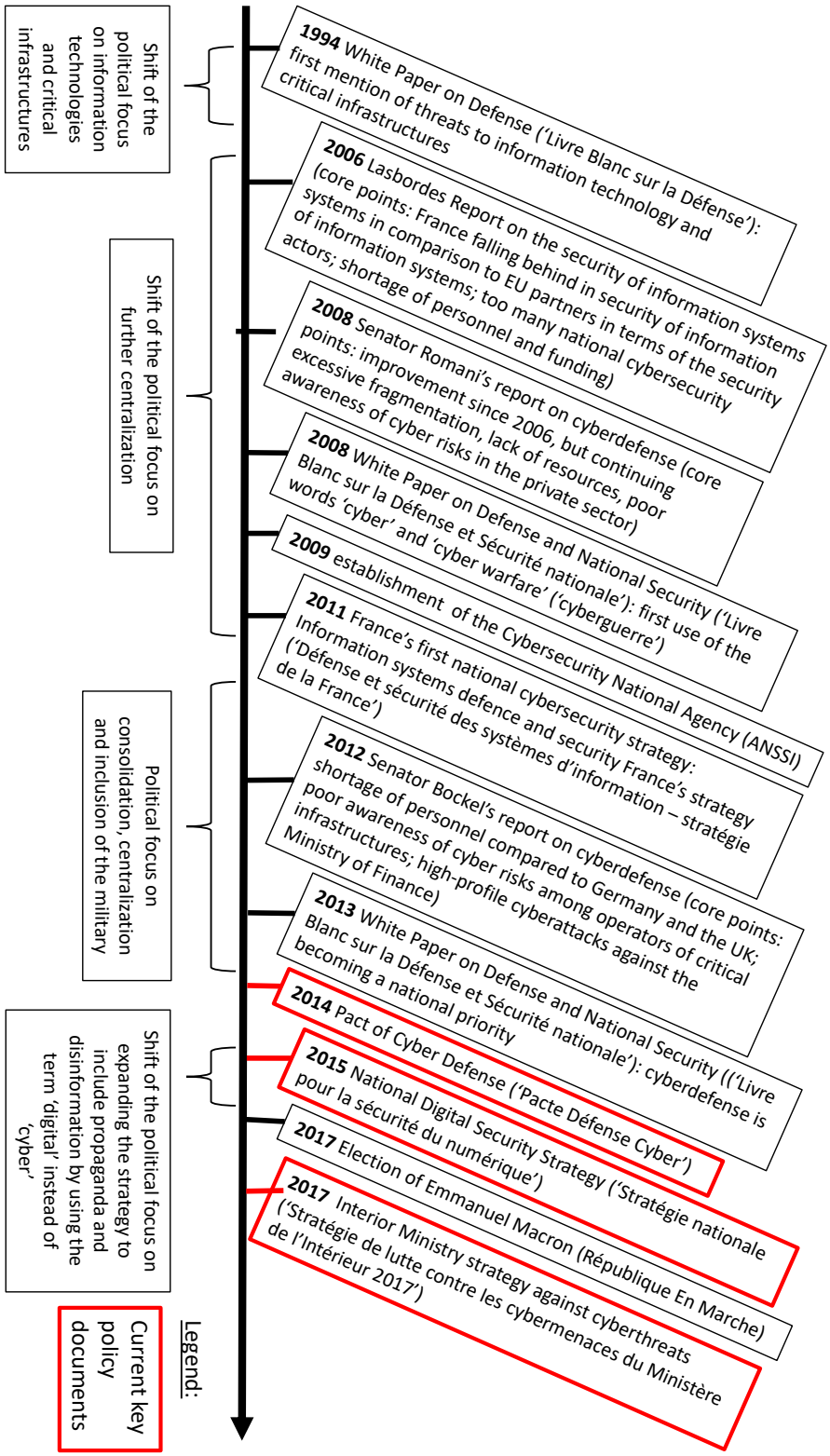
Cybersecurity	Cybercrime	Cyber defense	Intelligence services
TK: - Collegial body for comprehensive security policy- Development, coordination and monitoring of the NCSS	**NBI:** - Fight against, investigation and prevention of cybercrime and online crime - Assessment of the risk situation created by cybercrime	**FDFC5 – cyber department:** - Protection of data networks and infrastructure management of services - Development of defensive and offensive cyber capabilities - Development, maintenance and dissemination of information on cyber defense and cyber threats	**SUPO:** - Intelligence service and counter-espionage
NCSC-FI: - Information and communication security - Operational support and response - Preparation of situation analyses	- Coordination and implementation of criminal law investigations between police, customs and border control authorities - Function as national and international cooperation center		**PVTIEDL:** - Military intelligence service and military counter-intelligence - Collection of geodata and meteorological data

3. Acronyms

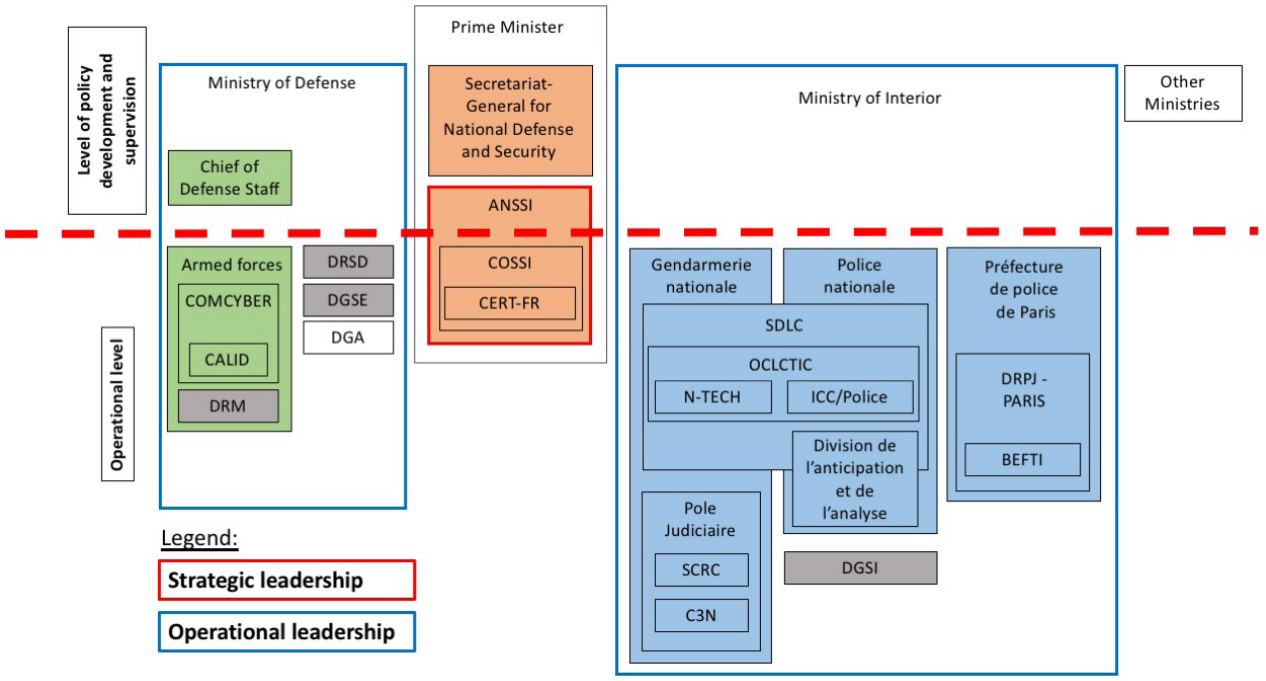
Acronym	Finnish	English
FDF	Försvarsmakten	Finnish armed forces
FICORA	Viestintävirasto	Finnish telecommunications regulatory authority
GOV-CERT	-	State CERT (IT emergencies)
GOVSITCEN	-	State situation center
HTAO	-	Office of the ambassador for hybrid threats
NCSA-FI	-	National Finnish authority for communication security
NCSC-FI	Kyberturvallisuuskeskus	National cybersecurity center
NCSS	Suomen kyberturvallisuusstrategia	National cybersecurity strategy
NESA/HVK	Huoltovarmuuskeskus	National crisis intervention authority
PVJJK/ FDFC5A	Puolustusvoimien johtamisjärjestelmäkeskus	Finnish armed forces – division C5
SUPO	Suojelupoliisi	Finnish security and intelligence service
TK	Turvallisuuskomitea	Security committee
UTVA	Valtioneuvoston ulko- ja turvallisuuspoliittinen ministerivaliokunta	Cabinet committee for foreign and security policy
VAHTI	Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä	State steering committee for information security
VALTORI	Valtion tieto- ja viestintätekniikkakeskus	State ICT center
YTS	Yhteiskunnan turvallisuusstrategia	Societal security strategy

Country information France

1. Core strategy documents and developments



2. Organization, main bodies and responsibilities



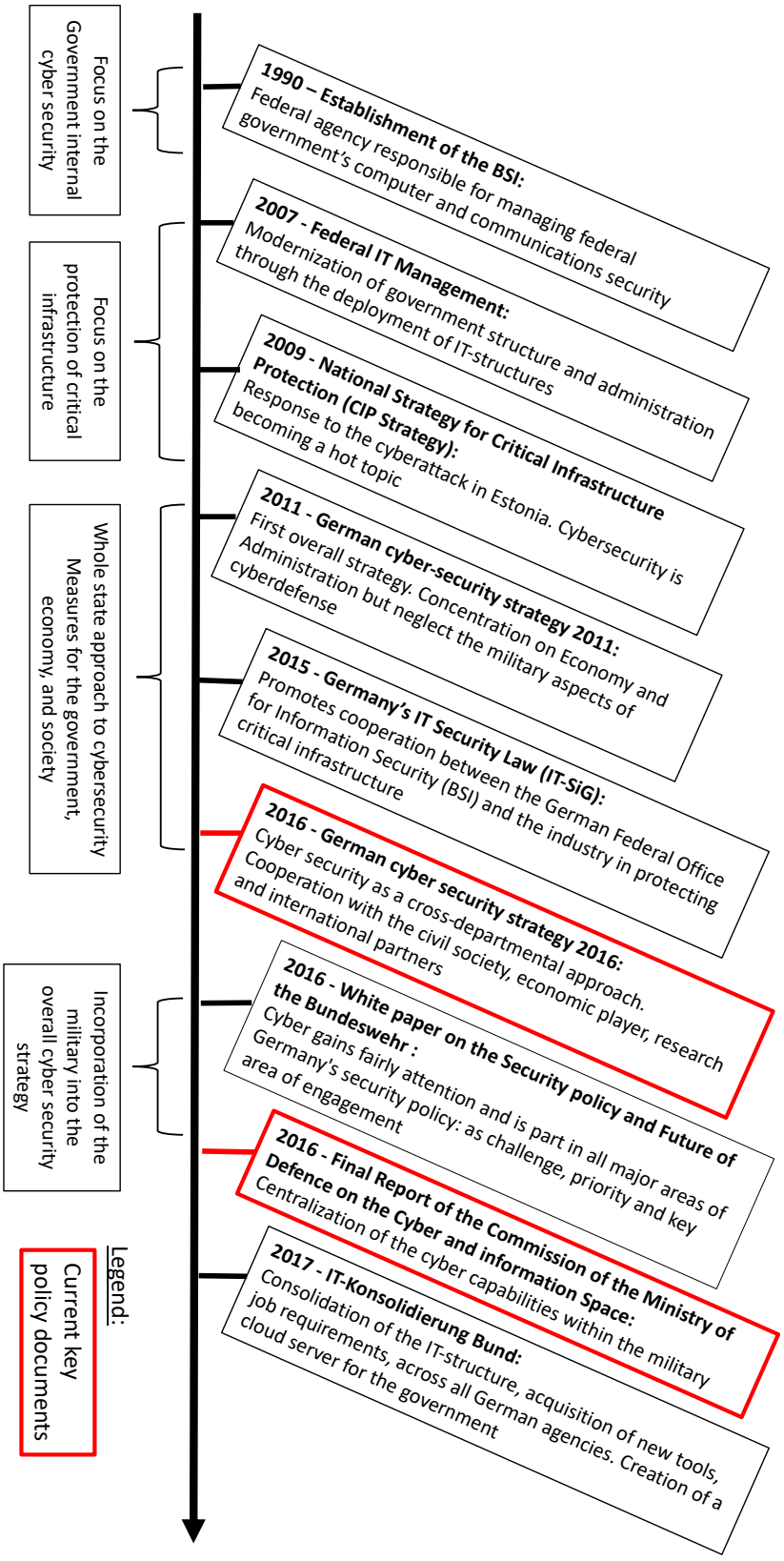
Cybersecurity	Cybercrime	Cyber defense	Intelligence services
ANSSI: - Centralization, coordination and government advice - Support for the private sector - Improvement of critical infrastructure security - Education, information, raising public awareness	**OCLCTIC:** - - Investigations relating to hacking, illegal contents and online fraud - Technical development - Education, information and expertise - National point of contact	**COMCYBER:** - Centralization and coordination of all bodies involved in cyber defense - Implementation of defensive and offensive cyber operations	**DGSI:** - Counterintelligence - Investigations of cyberattacks against critical and government infrastructures
COSSI: - Analysis of threats and system vulnerabilities - Development of responses to attacks - Provision of urgent technical support	**Anticipation and analysis department:** - Development of responses to cyberattacks on non-critical infrastructures - Raising public awareness of cyber threats	**CALID:** - Function as operational headquarters of the armed forces - Implementation and monitoring of cyber responses	**DGSE:** - Cyber surveillance
	C3N: - Education, information, training, research, monitoring/surveillance and investigation		**DRM:** - Military intelligence service
			DRSD: - Protection of personnel, information, materials and infrastructure - Monitoring of cyberspace - Counterespionage - Awarenessraising

3. Acronyms

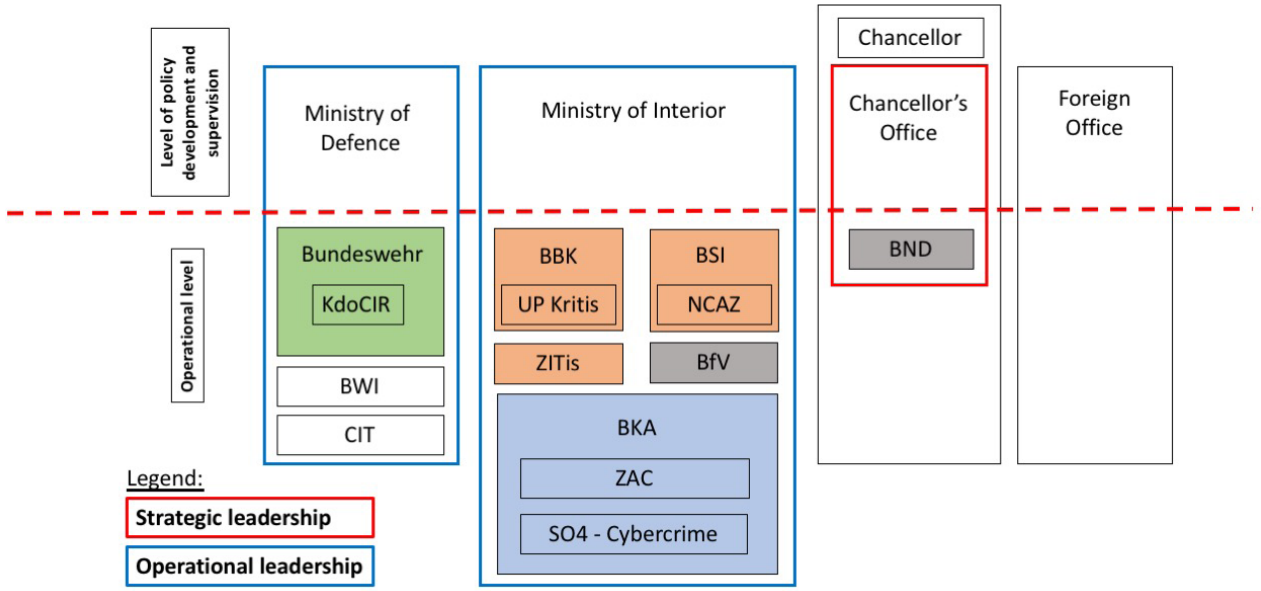
Acronym	French	English
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information	National cybersecurity agency
BEFTI	Brigade d'Enquête sur les Fraudes aux Technologies de l'Information	Investigation brigade for fraud and information technologies
C3N	Centre de lutte contre les Criminalités Numériques	Center against digital crime
CALID	Centre d'Analyse de Lutte Informatique Défensive	Analysis center for defensive cyber operations
CERT-FR	-	French CERT (IT emergency response team)
COMCYBER	Commandement des Cyberdéfense	Cyber command
COSSI	Centre Opérationnel de Sécurité des systèmes d'Information	Operational security headquarters for information systems
CRAC	Centre de Recherche et d'Analyse du Cyberespace	Cyberspace research and analysis center
DCPJ	Direction Centrale de la Police Judiciaire	Central directorate of the criminal investigation department
DGA	Direction Générale de l'Armement	Directorate-general of defense procurement
DGSE	Direction Générale de la Sécurité Extérieure	Directorate-general of external security
DGSI	Direction Générale de la Sécurité Intérieure	Directorate-general of internal security
DRM	Direction du Renseignement Militaire	Military intelligence service directorate
DRPJ-PARIS	Direction Régionale de la Police de Paris	Regional police directorate for Paris
DRSD	Direction du Renseignement et de la Sécurité de la Défense	Directorate of intelligence services and defense security
ICC/Police	Investigateur en Cyber-Criminalité	Cybercrime investigation authority
OCLCTIC	Office Central de Lutte contre la Criminalité liée aux Technologies de l'information et de la Communication	Central authority for fighting information and communication crime
SCRC	Service Central du Renseignement Criminel	Central bureau of criminal investigation
SDLC	Sous-Direction de la Lutte contre la Cybercriminalité	Anti-cybercrime division

Country information Germany

1. Core strategy documents and developments



2. Organization, main bodies and responsibilities



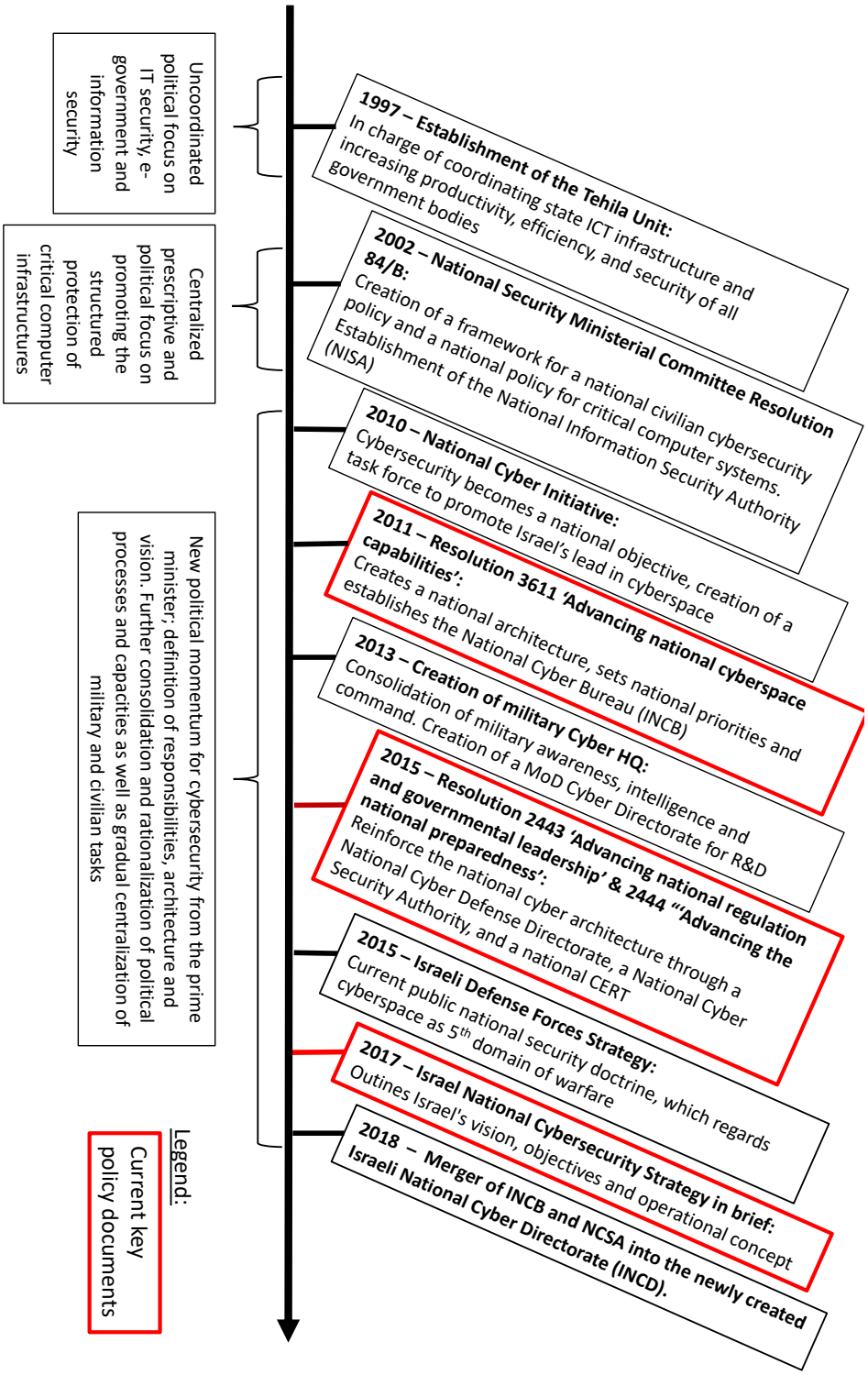
Cybersecurity	Cybercrime	Cyber defense	Intelligence services
Chancellery: - Central authority for cyber defense and security policy	**ZAC:** - Central contact point for cybercrime matters	**KdoCIR:** - Support for the protection of critical infrastructures - Development of defensive and offensive capabilities - Implementation of computer network operations (CNO) and electronic warfare tasks - Investigation of propaganda and disinformation - Gathering of military intelligence and assessment of cyber risks	**BfV:** - Intelligence service and counter-espionage - Maintenance of a mobile response team
BSI: - Information security and protection of state IT - Operational support and incident response - Development of the NCSS			**BND:** - Intelligence service - Cyber espionage and counter-espionage
NCAZ: - Joint defense platform of various civilian and military bodies - Sharing of information - Gathering of intelligence - Risk assessment	**SO4 – Cybercrime:** - Investigation - National and international cooperation center		
ZITis: - IT governance			
BBK: - Protection of critical infrastructures - PPP with operators of critical infrastructures			

3. Acronyms

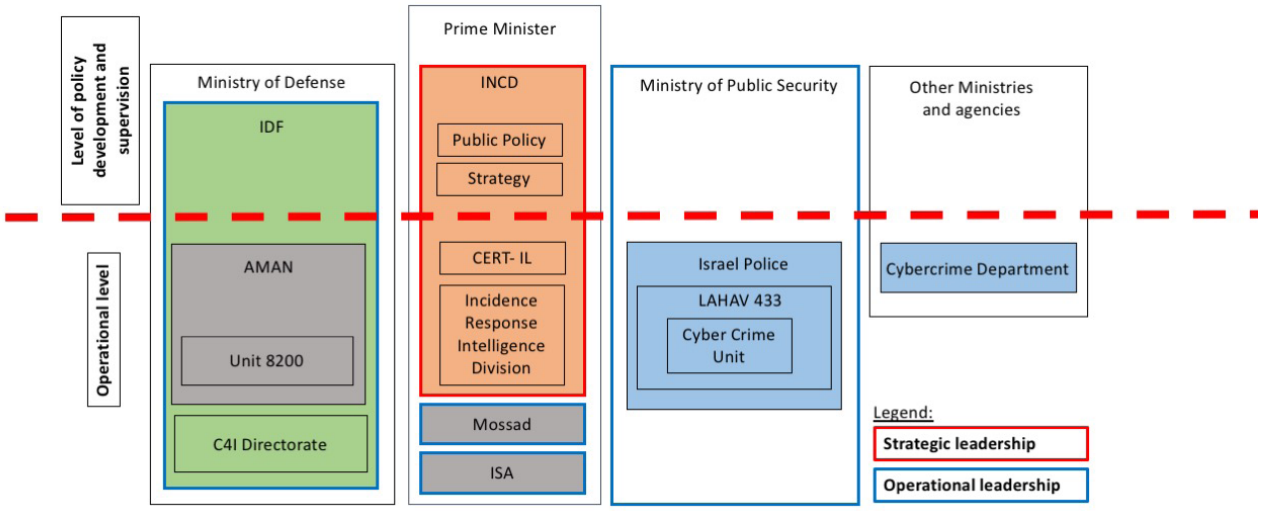
Acronym	German	English
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	Federal office for civil protection and disaster relief
BfV	Bundesamt für Verfassungsschutz	Federal office for the protection of the constitution
BKA	Bundeskriminalamt	Federal bureau of criminal investigation
BMI	Bundesministerium des Inneren	Federal ministry of the interior
BMVg	Bundesministerium der Verteidigung	Federal defense ministry
BND	Bundesnachrichtendienst	Federal intelligence service
BSI	Bundesamt für Sicherheit in der Informations-technik	Federal office for information security
-	Bundeswehr	Federal armed forces
BWI	Bundeswehr Informationstechnik GmbH	IT company of the armed forces
CIT	Abteilung Cyber/ IT	Cyber/IT division
Cyber-AZ	Nationales Cyber-Abwehrzentrum	National cybersecurity defense center
KdoCIR	Kommando Cyber- und Informationsraum	Cyber and information space command
NCAZ	Nationales Cyber-Abwehrzentrum	National cybersecurity defense center
SO4-Cyber-crime	Gruppe SO 4 – Cybercrime der Abteilung Schwere und Organisierte Kriminalität (SO)	Group SO 4 – cybercrime of the serious and organized crime division (SO)
UP Kritis	Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen	PPP for the protection of critical infrastructures
ZAC	Zentrale Ansprechstelle Cybercrime	Central cybercrime unit
ZITis	Zentrale Stelle für Informationstechnik im Sicherheitsbereich	Central authority for information technology in security

Country information Israel

1. Core strategy documents and developments



2. Organization, main bodies and responsibilities



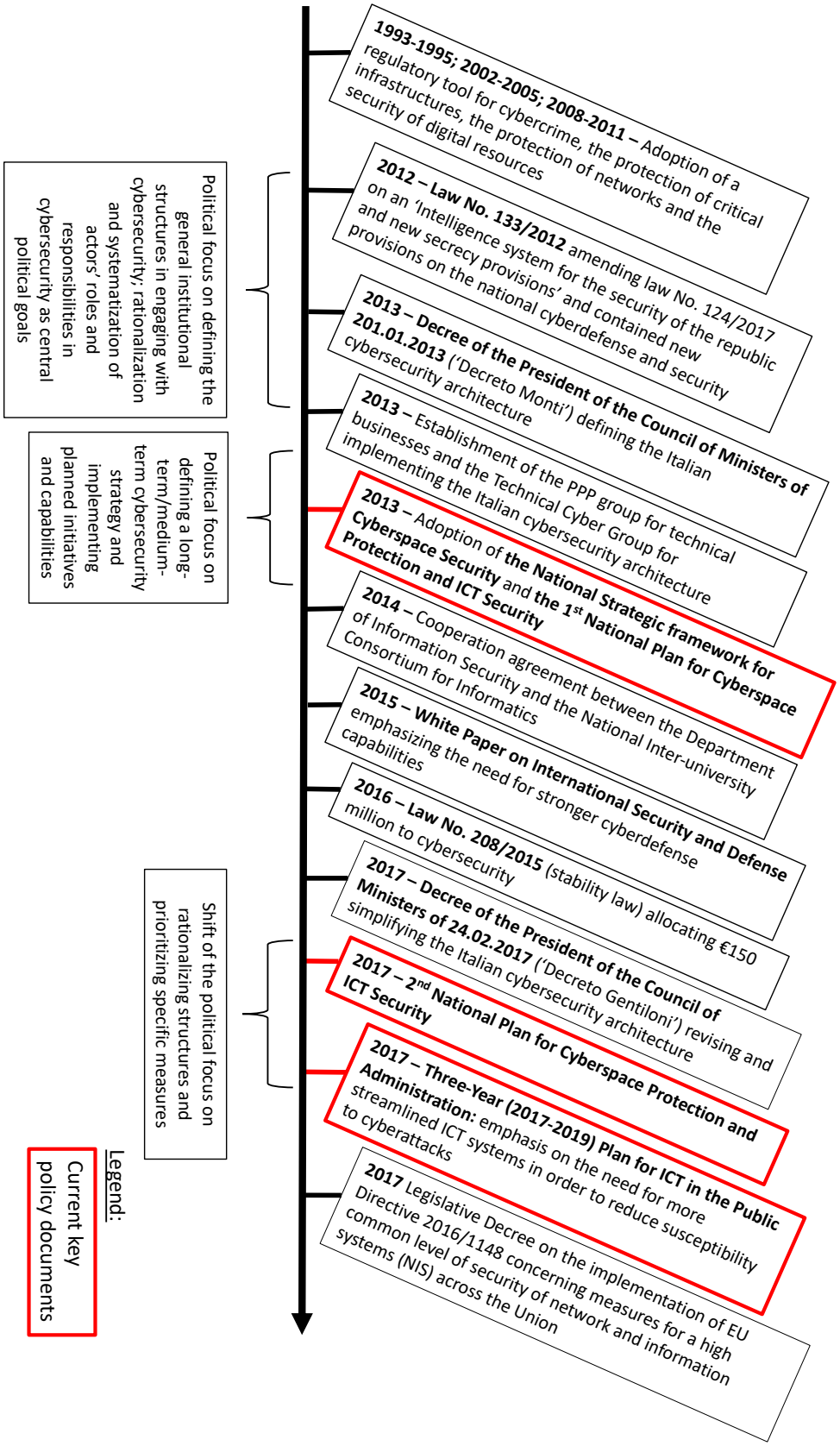
Cybersecurity	Cybercrime	Cyber defense	Intelligence services
INCD: - Development, coordination and implementation of the NCSS - Conduct and implementation of operational civilian defense activities - Advice to the prime minister and other authorities - Protection of critical information infrastructures	**LAHAV 433:** - Investigation, combat and prevention of cybercrime - Development of digital forensic expertise and capabilities - Criminal law investigations - Technical support for police units and investigators	**Directorate C4I:** - Coordination and implementation of defensive, proactive and offensive cyber operations - Coordination of cyber defense initiatives of the IDF - Protection of own infrastructures, systems and networks - Promotion and extension of education, information and competences regarding cyber defense	**AMAN:** - Gathering and processing of military intelligence - Conduct of military action in cyberspace (unit 8200) **ISA:** - Internal security and intelligence service - Counter-espionage and espionage
CERT-IL: - Incident management - Exchange of intelligence - Best practice for cybersecurity - Awareness-raising - Point of contact in case of threats			**Mossad:** - Intelligence service - Secret operations, counter-terrorism

3. Acronyms

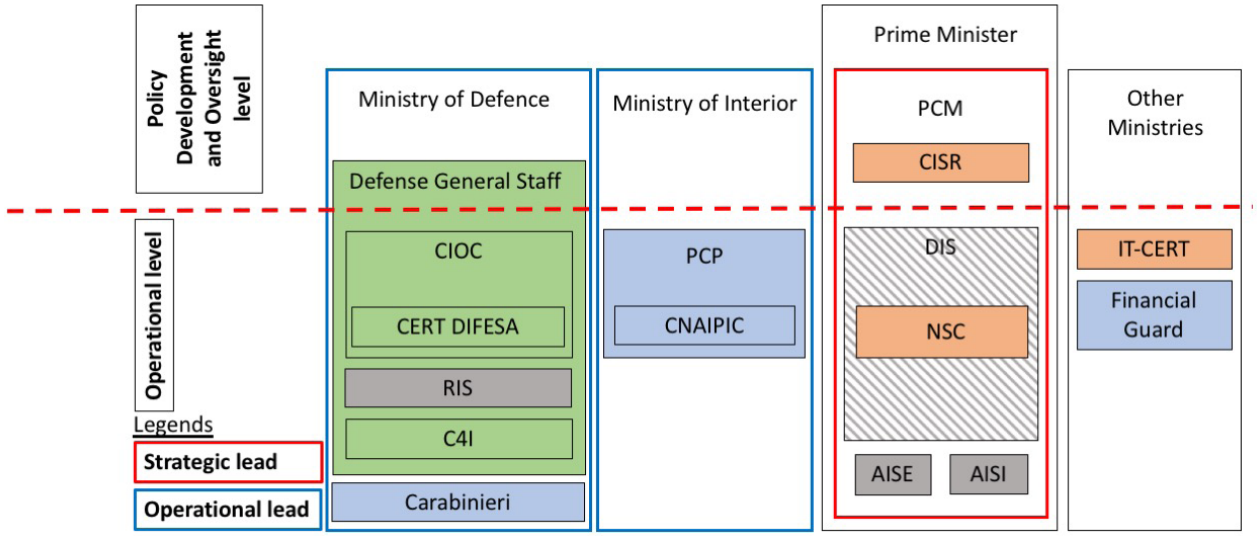
Acronym	Hebrew	English
AMAN	Agaf HaModi'in	Military intelligence service directorate
CERT-IL		Israeli national CERT (IT emergency response team)
IDF	Tsva ha-Hagana le-Yisra'el	Israeli armed forces
INCB		National cyber authority
INCD	Ma'arach	Israeli national cyber directorate
ISA	Shabak/Shin Beth	Israeli internal security agency
Maf'at	Maf'at	Administrative body for arms development and technical infrastructure
Mossad	HaMossad leModi'in uleTafkidim Meyuḥadim	Intelligence and special operations service
NCSA		National cybersecurity authority

Country information Italy

1. Core strategy documents and developments



2. Organization, main bodies and responsibilities



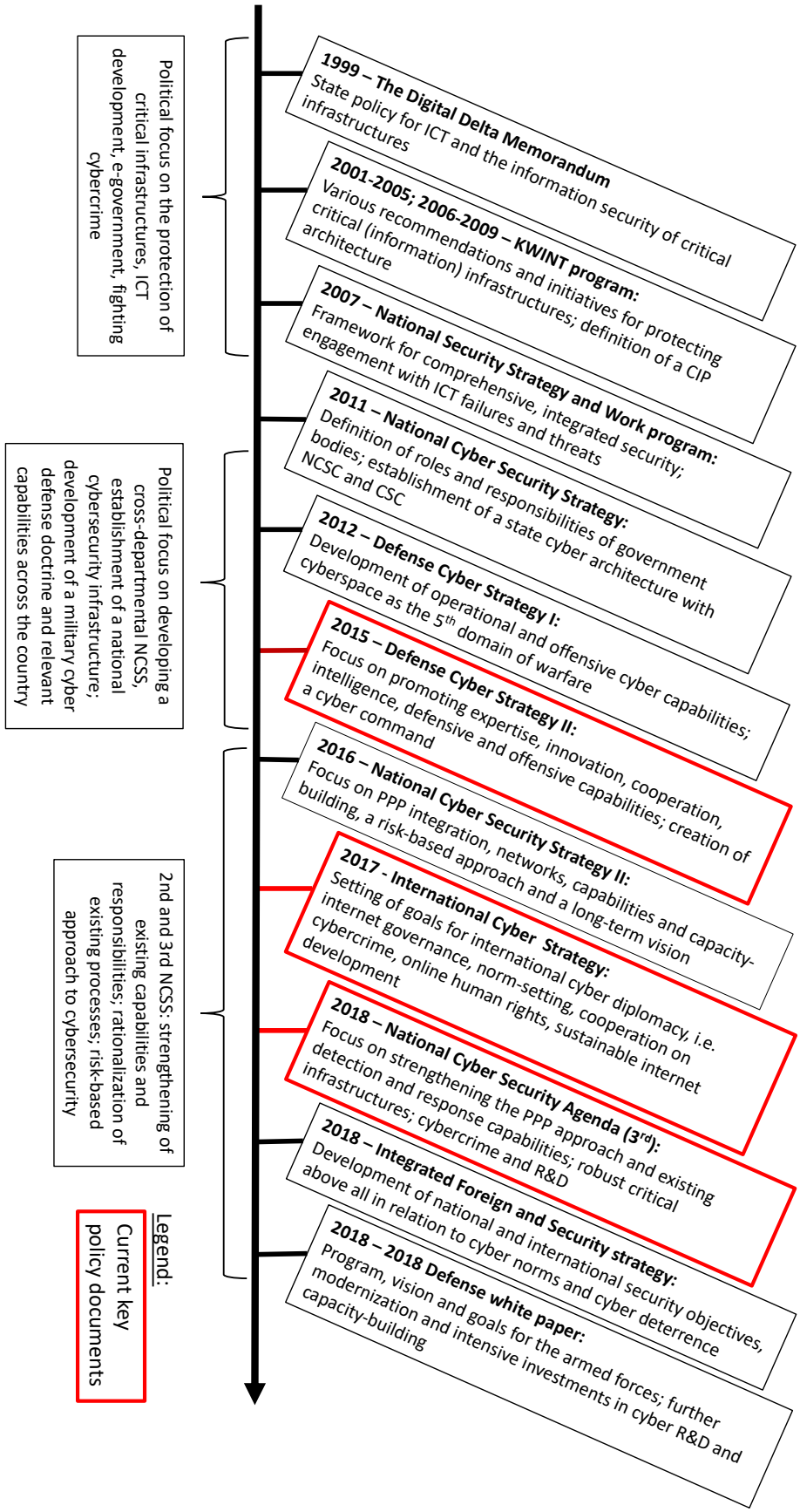
Cybersecurity	Cybercrime	Cyber defense	Intelligence services
NSC: - Coordination of government initiatives - Prevention, risk assessment, risk minimization, incident response and crisis management	**PCP:** - Fight against, investigation and prevention of cybercrime and online crime - Assessment of cybercrime and threats - Function as national and international cooperation center - Protection of critical infrastructures	**CIOC:** - Protection of military networks, services and infrastructures - Development of defensive and offensive cyber capabilities - Cyber defense situation analyses, threat assessment - Crisis response	**DIS:** - Coordination and exchange of intelligence - Risk assessment - Awareness-raising, education, information - National point of contact for cyber incidents
PCM: - Collegial body - Development, coordination and monitoring of the NCS	**Carabinieri:** - Investigation of telematics crime	**C4I:** - Operational planning and cyber operations - Command, control, telecommunications and ICT	**RIS:** - Military intelligence service and military counter-intelligence
CISR: - Advice on legislative issues and best practice - Promotion of cooperation, information exchange and PPP			**AISE/AISI:** - External/internal intelligence services and counter-espionage

3. Acronyms

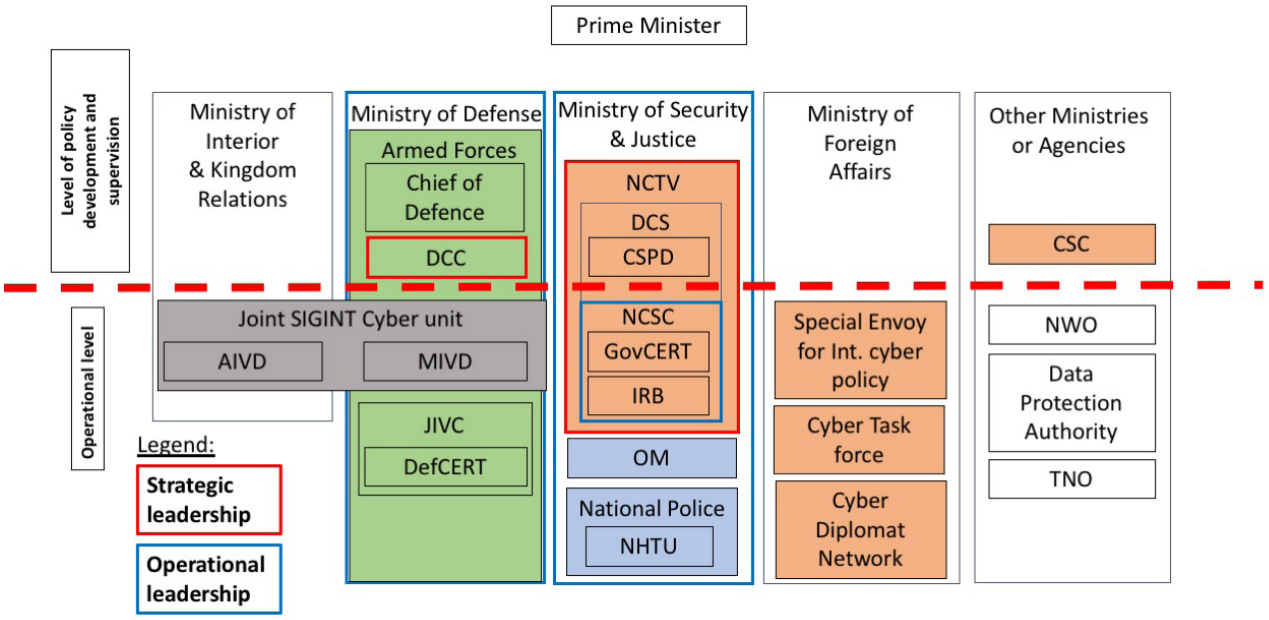
Acronym	Italian	English
AISE	Agenzia Informazioni e Sicurezza Esterna	External security and intelligence service
AISI	Agenzia Informazioni e Sicurezza Interna	Internal security and intelligence service
C4I	Comando C4 Difesa	Command, control, communications, computer and information systems division
CERT-DIFESA	Computer Emergency Response Team per le Forze Armate	CERT (IT emergency response team) for the armed forces
CERT-N	Computer Emergency Response Team Nazionale	Italian CERT (IT emergency response team)
CERT-PA	Computer Emergency Response Team per la Pubblica Amministrazione	CERT (IT emergency response team) for the public administration
CIOC	Comando Interforze Operazioni Cibernetiche	Joint command for cybernetic operations
CISR	Comitato Interministeriale per la Sicurezza della Repubblica	Interministerial committee for the security of the republic
CNAIPIC	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche	National anti-crime information center for the protection of critical infrastructures
DIS	Dipartimento delle Informazioni per la Sicurezza	Information security department
IT-CERT	-	Italian CERT (IT emergency response team)
NSC	Nucleo per la Sicurezza Cibernetica	Cybersecurity unit
NP cyber	Piano nazionale per la protezione cibernetica e la sicurezza informatica	National plan for protection in cyberspace and ICT security
PCP	Polizia Postale e delle Comunicazioni	Post and communications police
PCM	Presidenza del Consiglio dei ministri	President of the council of ministers
RIS	Reparto Informazioni e Sicurezza	Information and security division

Country information Netherlands

1. Core strategy documents and developments



2. Organization, main bodies and responsibilities



Cybersecurity	Cybercrime	Cyber defense	Intelligence services
NCTV: - Security policy nexus - Risk assessment - Policy cluster - Promotion of resilience against cyberattacks	**NHTU:** - Prevention, investigation and criminal prosecution of ordinary, high-tech and online crime - National and international cooperation center - PPP for exchanging information with the finance and private sector	**DCC:** - Coordination of cyber operations, intelligence and development of defensive/offensive capabilities - Promotion and management of cyber expertise and information among the armed forces	**AIVD/MIVD – Joint Cyber SIGINT:** - Counter-intelligence - Cyber espionage and counter-espionage - Military intelligence service, assessment of cyber threats
NCSC: - Operational coordination and support in case of crises - Information, advice and knowledge center			
CSC: - PPP with advisory and supervisory functions regarding the NCSS - Awareness-raising, research and development		**JIVC** - Protection and monitoring of military networks, IT services and systems - Resilience/susceptibility assessment - Crisis response	

3. Acronyms

Acronym	Dutch	English
AIVD	Algemene Inlichtingen- en Veiligheidsdienst	General intelligence and security service
CSC	Cyber Security Raad	Cybersecurity council
CSPD	-	Cybersecurity policy division
DCS	-	Cybersecurity directorate
DCC	Defensie Cyber Commando	Defensive cyber command
DefCERT	-	Dutch defense CERT (IT emergency response team)
NCSC	Nationaal Cyber Security Centrum	National cybersecurity center
IRB	-	Committee for ICT deployments
JSCU	-	Joint SIGINT cyber unit
JIVC	Joint IV Commando	Joint organization for information management
MIVD	Militaire Inlichtingen- en Veiligheidsdienst	Military intelligence and security service
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid	National coordinator for security and counter-terrorism
NHTU	-	National body for fighting high-tech crime
NWO	Nederlandse Organisatie voor Wetenschappelijk Onderzoek	Dutch organization for science and research
OM	Openbaar Ministerie	Public-prosecutor's office
TNO	Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek	Dutch organization for applied scientific research

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.