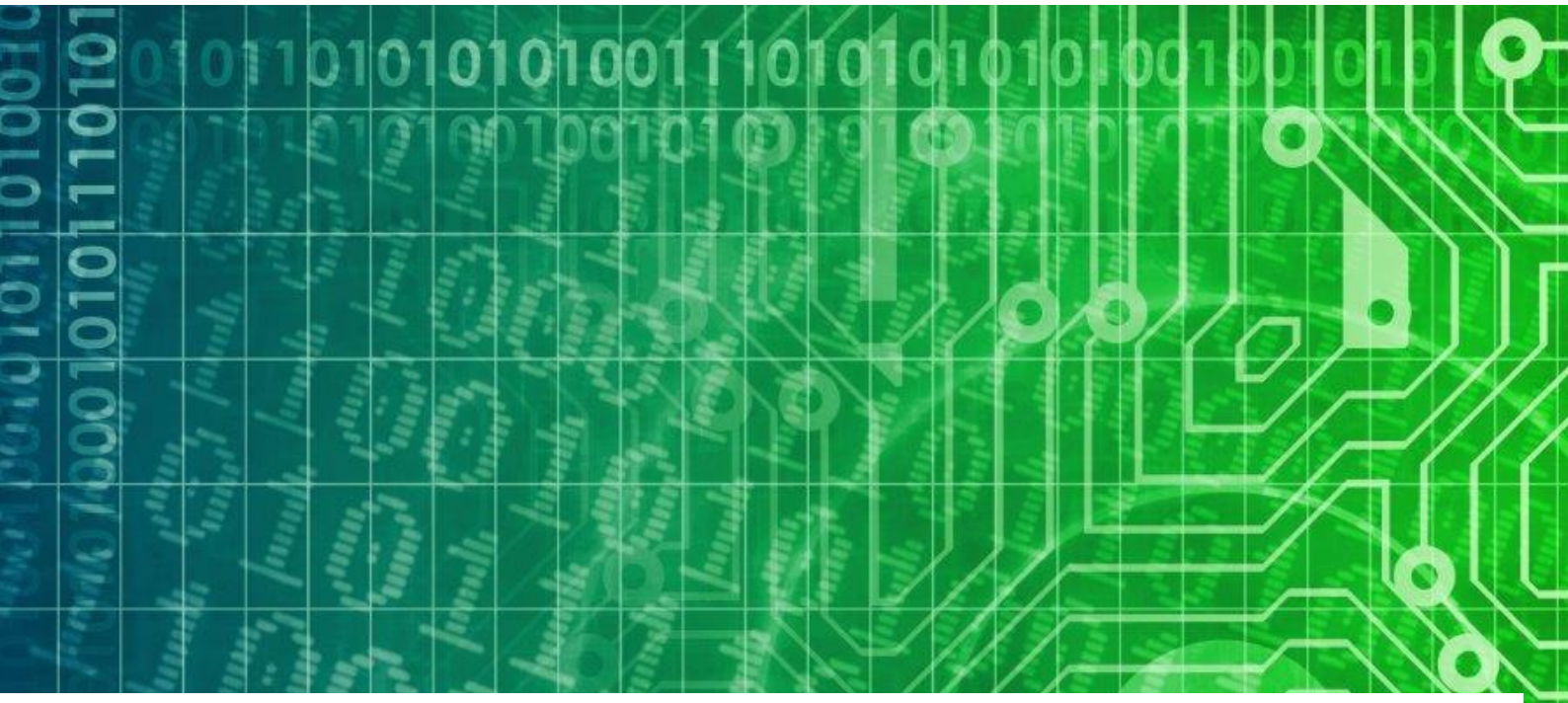
First Responder or Last Resort?

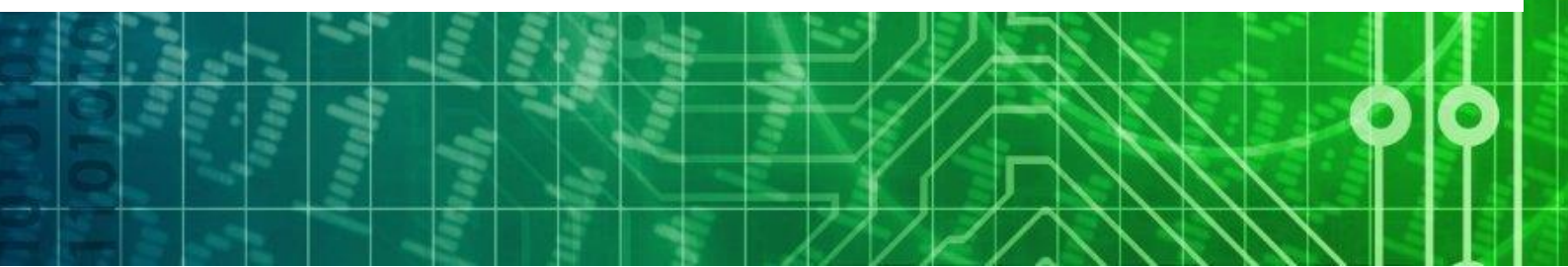
The role of the Ministry of Defence in national cyber crisis management in four European countries

Sergei Boeke

1 September 2016



Universiteit Leiden



Contents

1 Introduction

"An electronic Pearl Harbor" was waiting to happen, testified Winn Schwartau to the US Congress in June 1991. In the more than 25 years since, the analogy has been frequently reused by others, including a CIA director and the US Secretary of Defence, and it conjures up images of modern society grinding to a halt as a result of a targeted cyber attack.[1] As the debate on cyber conflict oscillates between alarmists and those that underplay the threat, cyber crises have come in different shapes and sizes. Some, like the Shamoon virus that struck the oil company Saudi Aramco in 2012, seriously impacted on business processes in a critical sector, while others like the Sony hack in 2014, threatened national security in a novel and unexpected way. But in the autumn of 2010, with the discovery of the Stuxnet worm, the international community realised what experts had already known for several years: that lines of code could lead to physical destruction, and that industrial control systems were particularly vulnerable to this new threat.[2]

On 23 December 2015 a power station in western Ukraine was hit by a well prepared, multi-stage cyber attack, leaving nearly a quarter of a million residents in the dark. Power was restored quickly, with the outage lasting between one and six hours. The manual back-up function proved vital, allowing the power station's operators to circumvent the automated systems that had their hard drives reprogrammed by the hackers. This manual function, however, is not always available in many modern Western power stations and grids.[3] The incident confirmed that vulnerabilities in critical infrastructure can still be exploited to great effect, and that malicious actors in cyberspace – many of whom state-affiliated – possess the capacity and intent to do so.

1.1 Defence

When the security of a nation is at stake, a natural reflex is to turn to the ministry of Defence. But should for instance the ministry of Defence or an intelligence service be responsible for securing national critical infrastructure, considering that in Western democracies most of this sector is held in private hands? It is an underlying principle in many Western states that individuals and individual organisations are first and foremost responsible for their own (cyber) security. Private-sector energy providers must therefore ensure a reasonable baseline of cyber security, keeping the simple hacker or cyber-crime group from disrupting such an important service. But should, for example, an electricity provider prepare for an adversary as capable and well equipped as the Russian FSB? This would entail

[1] Healey, *A Fierce Domain*, 33.
[2] For details, see Zetter, *Countdown to Zero Day*.
[3] Zetter, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid'.

a different risk assessment model, with considerable additional costs. This entails raising prices, which customers or regulators might be reluctant to accept, and it also leads to the *externality problem* (the organisation that must choose to apply security features does not suffer the primary costs of a security failure)[4]. Just as society has largely become dependent on the functioning of critical infrastructure (hence its prefix), different elements and sectors within critical infrastructure have become interdependent. As some previous outages have illustrated, an incident can trigger an unexpected cascade of failures, quickly developing into a crisis. The central government can thus become the problem owner of a crisis in the private sector, caused by a simple security breach or an accident.

Militaries and ministries of Defence are often seen as a last resort: when all else fails, they must keep going and save the day. As the largest pool of (public) cyber capacity is often vested in the military or intelligence agencies, it raises the question when and under what circumstances they should be mobilised in support of cyber crises. In April 2015, Eric Rosenbach, a U.S. assistant secretary of Defense, stated that "The Department of Defense is not here to defend against all cyber attacks -- only that top 2 percent – the most serious."[5] While this in no way answers when and under what circumstances U.S. Defense capacity should be used to support the civilian sector, Rosenbach did clarify that in the U.S., the Department of Defense *is* tasked with protecting critical infrastructure, and responding to the most serious cyber attacks. Choosing not to clarify the eventual role of Defence in crisis situations certainly bears a risk. In dire emergencies, a popular expectation that Defence can always fulfil the *ultimum remedium* role can lead to a request to the military to intervene and assist, whether they have a designated role or none at all. In the latter case this would imply a hasty improvisation on the part of the military.

Much of the debate on the role of the ministry of Defence in cyber crisis management is conducted on the premise of peacetime circumstances. The distinction between war and peace, or whether a state is in armed conflict with another state, is essential. The laws of war (*jus in bello*) dictate that warring states can only hit targets meeting the *military necessity* and *proportionality* criteria.[6] This means that under certain circumstances, power stations and other critical infrastructure can justifiably be targeted. During operations such as Allied Force (Kosovo 1999) and Operation Iraqi Freedom (2003), this is precisely what the allies did.[7] Cyber, however, would now allow an advanced adversary to hit back in the intervening state, and critical infrastructure would be an appealing target, especially compared to better protected military targets and networks. This would not only be an effective way for an embattled state to respond to a more powerful intervening nation, but if the criteria of military necessity and proportionality were respected, a cyber attack on critical infrastructure could in theory

[4] Bauer and van Eeten, 'Cybersecurity'.
[5] Marshall Jr., 'New DoD Cyber Strategy Nears Release, Official Says'.
[6] Boivin, *Legal Regime to Targeting Military Objectives*.
[7] Dinstein, 'Legitimate Military Objectives'; cf. Wall, *Lessons of NATO's Kosovo Campaign*; Knights, 'Operation Iraqi Freedom'.

even be regarded as legitimate and in accordance with international law. The United Nations Group of Governmental Experts has concluded that international law applies to cyberspace,[8] and the *Tallinn Manual* offers an interpretation of how different principles of humanitarian law could apply to cyber during times of conflict.[9]

The West has previously intervened in countries that had little or no cyber capacity for retaliation or resistance, but now many potential adversaries in conflict zones possess significant cyber capacity to do harm. Non-state actors, whether for example terrorists, patriotic hackers or 'hacktivists', could equally target an intervening country with cyber attacks. All this would imply that participating in a military intervention or peace-enforcing mission could endanger national critical infrastructure. This would either deter the state from conducting the military intervention in the first place, or if it does intervene, put the onus on the state and the military to provide extra protection to national critical infrastructure. An active and interventionist foreign policy, therefore, could necessitate a well-developed policy of national cyber defence.

1.2 Actors and interests

The field of cyber security is characterized by unclear definitions and the blurring of traditional boundaries. To avoid delving too deep into the debate on definitions, scope and domains, the few definitions used in this report are taken from the Dutch cyber security strategy or policy papers. The government defines cyber security as follows:

> Cyber security is freedom from danger or damage due to the disruption, breakdown, or misuse of ICT. The danger or damage resulting from disruption, breakdown, or misuse may consist of limitations to the availability or reliability of ICT, breaches of the confidentiality of information stored on ICT media, or damage to the integrity of that information.[10]

An ICT-crisis is defined as a crisis that has its origin in the IT-domain, impacts on one or more critical infrastructure sectors, where generic crisis management structures are insufficient for addressing it.[11] Not all countries have defined these and other important terms in their policies, but this report will note if significant differences were encountered between the definitions used here and those by different countries or organizations.

As for the blurring of boundaries, the most important vectors concern the public and private sector and national security and law enforcement. The public-private partnership (PPP) serves as the cornerstone of many national cyber security strategies, as neither domain is capable of addressing the challenges alone. Behind public displays of unity of effort, however, important diverging interests still lead to

[8] UN General Assembly, 'Report of the Group of Governmental Experts'.
[9] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*.
[10] Ministerie van Veiligheid en Justitie, *NCSS 1 [English Version]*, 4.
[11] Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Nationaal Crisisplan ICT*, 5.

significant problems that need to be addressed.[12] If the state does not deliver what the market demands, private companies will fill the void. This has been the case for cyber threat intelligence as well as technical crisis response, and a large private sector industry is now blossoming, led by companies like FireEye and Fox-IT. These companies often provide expertise that governments do not have, with a speed the public sector cannot meet. According to some, this new 'cyber-industrial complex' has far-reaching implications, but important for this report is the issue of *capacity*.[13] In many countries, IT-security companies often possess more capacity for crisis response than the state, giving them a primary role in crisis response.[14] The concept of public-private partnerships is not just relevant for defenders, but also for offence, with some countries like Russia having outsourced malicious cyber activities (e.g. espionage and sabotage) to non-state criminal groups.[15] Although it might not impact on crisis management, it certainly complicates incident response and blurs the boundaries between law enforcement and national security. According to the Estonian Information System Authority:

> In cyberspace, it is progressively challenging to differentiate between criminals that are motivated by personal gain and the security services of a neighbouring state that are interested in employing hybrid warfare against Estonia in pursuit of national objectives. [16]

When reacting to an IT-incident – before it has turned into a crisis - different responding actors can have diverging interests. A service provider who has been the victim of a hack or intrusion, will generally desire to overcome the disruption as quickly as possible and restore the provision of services. The police, when they come across a crime scene, will aim to keep the evidence intact and uncontaminated, to be able to track and prosecute the perpetrators. The law enforcement approach can entail physically removing terminals or servers to be able to start the forensic investigation. Conversely, when an intelligence agency is involved, their natural reflex is to keep state-sponsored intruders in the system, to observe their modus operandi and learn more about their actions and intentions. This policy choice means that the first responder must act stealthily, so as not to reveal to the intruders that they have been detected, which could cause them to rapidly dismantle their attack infrastructure. After sufficient intelligence has been gathered, the intruders can then be expelled on the terms of the defenders. These conflicting approaches can complicate the policy of incident response, with potential for the policy to be set by the organization that arrives 'on the scene' first.[17]

[12] Carr, 'Public-Private Partnerships in National Cyber-Security Strategies'.
[13] See for example Harris, *@WAR*.
[14] Stone and Riley, 'Mandiant, the Go-To Security Firm for Cyber-Espionage Attacks'.
[15] Corera, *Intercept*, 287.
[16] '2015 Annual Report of the Estonian Information System Authority's Cyber Security Branch', 5.
[17] Luiijf, principal consultant at TNO, interview.

1.3 Crisis management

In the academic literature on crises, there are many differing definitions of what constitutes a *crisis*, but they contain three ubiquitous elements: time pressure, a serious threat, and a high level of uncertainty (both on what the situation is, and how it may unfold).[18] When these three features are present, the regular decision-making process may no longer prove effective. Countering the common assumption that decision-making during crises becomes more centralized, Paul 't Hart et al. illustrated in an old but still relevant article that other forms of decision making are possible, and that these can be more effective than the classic centralised top-down model.[19] These possibilities include informal decentralization or non-decision making, and have been confirmed by much of the research since then.[20]

Crisis management literature also transcends incident response, and crises are increasingly viewed not as events, but as processes.[21] It then becomes apparent that a crisis is built up over time, with cumulating imperfections and warning signals missed, leading up to a *triggering event.*[22] To successfully manage (future) crises, focus should therefore not be restricted to the phase where an incident occurs, but equally on the preceding and following developments. Many different models and distinctions are being used in this field. One such model distinguishes five phases for effective (cyber) crisis management: prevention, preparation, containment, recovery, and learning.[23] Others propose less sequential models, where the phases are not mutually exclusive.[24] When applying these models to cyber security, the 'cyber' element can be present in any or all of the phases. It is therefore essential to know which phases require a specific 'cyber' approach, to effectively prevent or deal with a crisis.

1.4 Scope and methodology

This report will investigate the role that the ministry of Defence plays in cyber crisis management in four small-to-medium-sized European countries. What role does Defence play in national cyber security and are there any specific provisions for providing assistance during cyber crises? The situation in Netherlands, where this study was commissioned, is studied first to provide a frame of reference. Denmark was chosen as one of the comparative cases, as its ministry of Defence plays a central role in cyber security as well as national crisis management. Denmark is characterized by its strong Atlantic outlook (focus on the US and UK), a security policy strongly embedded within NATO,

[18] Boin, *Crisis Management*; 't Hart, Rosenthal, and Kouzmin, 'Crisis Decision Making'.
[19] 't Hart, Rosenthal, and Kouzmin, 'Crisis Decision Making'.
[20] Ibid.; Boin and Bynander, 'Explaining Success and Failure in Crisis Coordination'; Boin and 't Hart, 'Organising for Effective Emergency Management'; Boin and McConnell, 'Preparing for Critical Infrastructure Breakdowns'; Pearson and Clair, 'Reframing Crisis Management'; Dynes and Aguirre, 'Organizational Adaptation to Crises: Mechanisms of Coordination and Structural Change'.
[21] Pearson and Clair, 'Reframing Crisis Management'; Roux-Dufort, 'A Passion for Imperfections'.
[22] Roux-Dufort, 'A Passion for Imperfections', 226–27.
[23] Kovoor-Misra and Misra, 'Understanding and Managing Crises in an "Online World"'.
[24] 'A Passion for Imperfections: Revisiting Crisis Management', 243–245: 1.

but with an opt-out from the EU. The third case for the study is Estonia, which has been a prominent leader on cyber policy since it was a victim of large scale DDoS attacks in 2007, although its focus on e-governance and cyber predated the crisis. Finally, the Czech Republic complements the list, as this country has been busy developing national cyber security, also with the ambition of becoming a leading cyber power in the region and beyond. Since cyber crisis management is broader than incident response, each chapter starts with mapping the governmental institutions responsible for coordinating and implementing national cyber policy, before focusing specifically on Defence. Subsequently, the national crisis management structures are described, particularly *if* and *how* cyber plays a specific role. The final chapter provides an analysis of the findings, identifying some variables that can be used to categorize national policy choices and elaborating on some of the unique features of each country.

This study is designed as a comparative case study, and uses literature review complemented by document analysis and semi-structured interviews. For each country, the roles and responsibilities of government ministries are well described in public documents, and each country has also published its cyber security strategy in English. For some countries, good overviews of national institutions and their specific cyber roles are already provided by NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE). However, while structures and strategies are available in public documents, there is much less open source information available that provides insight into the way things work out in practice, from implementation to information sharing. Much of cyber security is still shrouded in secrecy, with defenders and victims loath to disclose information on vulnerabilities and breaches, and intelligence agencies reluctant to share classified material.[25] To bridge this gap between practice and research, the author has conducted many interviews with officials from national cyber security organisations. Due to their positions in the respective national security structures, the interviewees have requested to remain anonymous. Their insights have nevertheless provided invaluable input for the analyses and conclusions. The country sections have also been checked for factual correctness by officials responsible for those sectors, although the analysis and conclusions at some points diverge from official standpoints.

[25] Libicki, Ablon, and Webb, *The Defender's Dilemma Charting a Course Toward Cybersecurity*.

2 The Netherlands

The Dutch government's cyber policy was in part initiated by a motion tabled by two members of Parliament in 2010. Their primary concern was the lack of an integrated cyber policy and the absence of cyber in the Defence budget, and they proposed that Defence would coordinate and lead the cyber crime and defence policy.[26] At the time, the Ministry of Security and Justice had already garnered ideas and input from a broad scope of public and private stakeholders, and in early 2011 the country's first National Cyber Security Strategy was published. The strategy focussed on improving digital awareness, building capacity and investing in resilience.[27] Individual responsibility (for users as well as organizations), combined with the public private partnership model, formed the two cornerstones of the strategy. This was articulated as self-regulation where possible, laws and rules where necessary. The ministry of Security and Justice would coordinate cyber policy, and a new Centre for Cyber Security (*Nationaal Cyber Security Centrum*: *NCSC*) was to be embedded in it. On a strategic and advisory level, an independent Cyber Security Council (*Cyber Security Raad*) was also established, consisting of highly placed representatives of public and private parties (seven seats each) and the scientific field (four seats). Their task is to provide solicited and unsolicited advice to the government on cyber security, and with their multi-disciplinary angle they do not just focus on threats, but also on social and economic opportunities.[28] At the end of 2013, the National Cyber Security Strategy 2 was published. This shifted the focus from awareness to capability, public private partnership to public private participation and from structures to networks and coalitions.[29]

The so called *polder model*, a consensus guided approach involving all stakeholders, seems ingrained in society and has contributed to governance through and with network organizations. Both before, during and after crises, such organizations serve to bring relevant parties together, and maintain connections with other clusters. The NCSC forms the central hub for different networks and 'cooperative alliances'. Mainstreaming cyber implies that existing institutional and sectoral lines are largely followed, and that a myriad of government organizations have developed their own cyber security capacity. A historical wariness of central authority and resistance to centralization have led to a culture that facilitates network alliances, consensus decision-making and community building. This is reflected in an effective Dutch public private partnership model, but equally a somewhat fragmented landscape with cyber capacity spread over different organizations and ministries. Next to a high tech crime unit in the police force, the Koninklijke Marechaussee (equivalent to a Gendarmerie)

[26] *Motie Hernandez en Knops*, Tweede Kamer 2010-2011, 32 500 X, nr. 76.
[27] Ministerie van Veiligheid en Justitie, *NCSS 1 [English Version]*.
[28] Cyber Security Raad, *CSR - Cyber Security Raad*.
[29] Ministerie van Veiligheid en Justitie, *NCSS 2*.

investigates cyber intrusions/crimes against Defence, as well as those committed by military personnel. Much of the Kmar's capacity is dedicated to law enforcement, and thus falls under the remit of the ministry of Security and Justice. There is close cooperation with the police on this task, and both organizations investigate document and ID-fraud on the Internet. Next to the KMar, there are several other units within Defence investing in cyber capacity: the Defence CERT, the Defence Cyber Command, and the Joint Sigint Cyber Unit. The ministry of Defence also published its own Defence Cyber Strategy in 2012 (updated in 2015) and, recognizing cyberspace as a fifth domain, is planning to operationalize cyber in its combat capacity.[30]

2.1 Institutions/organizations

The National Cyber Security Centre, created in 2012, is the central coordinating authority on national cyber security in the Netherlands. It is embedded within the National Coordinator for Security and Counterterrorism (NCTV), which in turn is part of the Ministry of Security and Justice.[31] The NCSC incorporated the former GovCERT, but is not tasked with actually monitoring public IT-networks. Rather, it has an active coordinating role, in the preventive and reactive phases of incidents and crises, forming the central government node. As mentioned in the Netherlands first and second National Cyber Security Strategies, there is a strong emphasis on individual responsibility, from a personal as well as organizational point of view. Known as the subsidiarity principle, each user and organization is responsible for its own cyber security and/or networks. This therefore also applies to the various government ministries. They are responsible for the security of their own networks, and contract *Security Operation Centres* (SOCs) either in house or through IT-service providers. With the second Cyber Security Strategy, the NCSC's role was expanded to also serve as a CSOC to inform and warn other SOCs.[32]

Rather than imposing central authority that monitors IT-networks, there is a cooperative network approach in which different parties in the public and private sector cooperate and share detection data. In 2013, the NCSC launched the National Detection Network (NDN). This system serves many – but not all – of the central government (ministries) and parts of the critical infrastructure sector. Several sensors in government networks detect anomalies and malicious traffic, which are fed by a database of indicators of compromise (IOC). The General and Military Intelligence and Security Agencies (AIVD and MIVD) provide input and operate on possible intrusions. As a result, targeted organizations are informed of attacks against their networks, and can cooperatively take appropriate defensive measures. The system probes analyse traffic and the IOCs provided by the intelligence community ensure a level

[30] Ministerie van Defensie, 'Actualisering Defensie Cyber Strategie'; Luijf, 'The Netherlands'.
[31] 'Organization', *Nationaal Cyber Security Centrum*, accessed 22 April 2016, https://www.ncsc.nl/english/organisation.
[32] Senior officials at the National Cyber Security Centre, Interview.

of detection that exceeds what commercial anti-virus software offers. However, the NDN only provides advance warning of cyber threats, and cannot investigate the source of the attacks. Information on who has been attacked, and how, can sometimes not be shared.[33] The system relies on a significant input of the intelligence services, which cannot always be shared due to the classified nature of certain data. As a result of these and other restrictive legal factors, intelligence officials consider the NDN ineffective against sophisticated APTs.[34] Two other systems, Taranis and Beita are also deployed by the NCSC. Taranis is a bespoke software application that helps streamline internal processes concerning advisories that are sent to users, while Beita employs honeypots to lure attackers into fake target environments.[35]

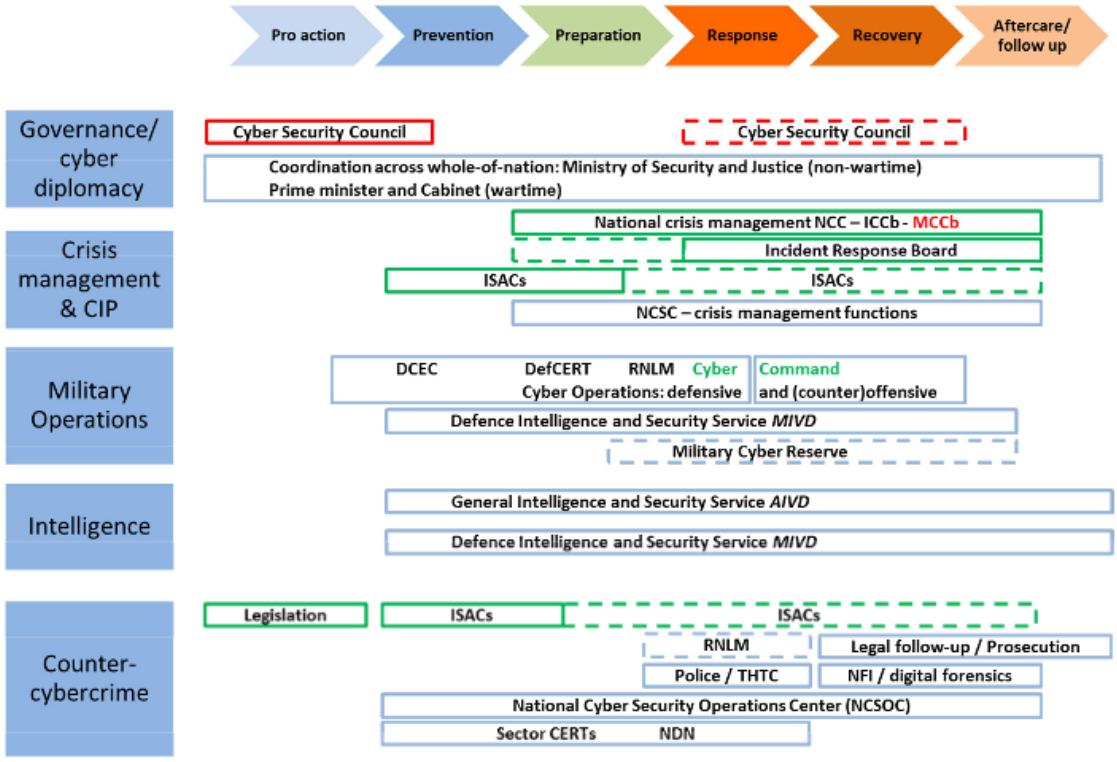


Figure 2.1 The Dutch cyber-conflict response structure36

The NCSC plays a central role in information sharing. It is a member of several national and international sharing platforms, some involving exclusively public sector organizations while others also include private sectors instances. Within the Netherlands, the NCSC organizes the Operational Incident Response Team Forum (Operationeel Incident Response Team Overleg, O-IRT-O), a

[33] Ministerie van Veiligheid en Justitie, 'Presentatie Nationaal Detectie Netwerk'.
[34] Senior officials at the MIVD and JSCU, interview.
[35] National Cyber Security Centre, 'Taranis: Turning Your Sources into Reusable Security Alerts', 12 February 2014, http://www.nisha-network.eu/sites/default/files/20140212-NISHA-workshop-Taranis.pdf ; 'Beita', *Nationaal Cyber Security Centrum*, accessed 2 June 2016, https://www.ncsc.nl/english/Incident+Response/monitoring/beita.html.
[36] As appeared in Luiijf, 'The Netherlands'; based on Luiijf and Healey, 'Organisational Structures & Considerations'.

collaboration of Dutch CERTs from both the public and private sector, where operational information is shared.[37] In the international field, the NCSC represents the Netherlands in the International Watch and Warning Network (IWWN). This platform unites government representatives of 15 countries, ranging from Japan to Switzerland and the US.[38] Sensitive information is shared, representatives and dossier holders can establish point-to-point contacts with their counterparts in member countries, and exercises and training are promoted. More technical and operational information for incident response is garnered from the NCSC's membership of the European Government CERTs (EGC) group. Finally, the NCSC is a member of the Forum of Incident Response and Security Teams (FIRST), a global network of public and private CERTs that exchange information and best practices.

In the field of awareness, preparation and prevention, the NCSC publishes several different types of reports. On a strategic level, the annual *Cyber Security Assessment Netherlands* gives a (predominantly retrospective) overview of the developments and threats in cyberspace. The document is drawn up in close collaboration with several public and private parties,[39] and is therefore a consensus document. The security and intelligence services participate in the drafting process, but do not contribute detailed analyses of specific threats and are wary of attributing specific past attacks, leading to some experts questioning the value of the reports.[40] On an operational and technical level, the NCSC publishes around 2000 advisories a year, specifically aimed at highlighting discovered vulnerabilities. These advisories are categorized according to a risk analysis model, estimating the probability of occurrence and the potential impact or damage that can be caused. Much of the information incorporated in these Dutch language reports is from software vendors and comes from the information-sharing networks that the NCSC is a member of. Other NCSC publications include factsheets, white papers and dossiers, the latter concerning and detailing large-scale incidents or crises.[41] The NCSC also facilitates the responsible disclosure file, offering different sectors guidelines for the procedure. If necessary, the NCSC can play an intermediary role between the reporter and the notified organization, and if the vulnerability concerns a government network or system, the NCSC coordinates the process.[42]

Sharing with other organizations, however, remains an activity that is rooted in trust relationships. Like sharing in the intelligence world, it is often based on protecting operational sources and not compromising your own organization/country's information position. Sharing is thus based on a quid pro quo understanding, and the larger the sharing circle, the less sensitive - and valuable – the shared

[37] Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Nationaal Crisisplan ICT*.
[38] Estonia, the Czech Republic and Denmark – the other countries studied for this report – are not members of the IWWN.
[39] Ministerie van Veiligheid en Justitie, *NCSS 2 [English Version]*; Algemene Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2015*.
[40] Broeders, *Investigating the Place and Role of the Armed Forces in Dutch Cyber Security Governance*, 23–24.
[41] 'Expertise & Advice', *Nationaal Cyber Security Centrum*, accessed 2 June 2016, https://www.ncsc.nl/english/expertise--advice.
[42] Senior officials at the National Cyber Security Centre, Interview.

information is. The sharing of sensitive information – either concerning sophisticated state-sponsored cyber threats or important vulnerabilities - is often done bilaterally or in small trusted communities. The main barrier for sharing is located between the international intelligence communities and the cyber security centres that are outside this sector. As the NCSC is placed outside the intelligence community, the Dutch intelligence services do not share much information with the NCSC that they receive from their international partners, including the cyber security centres that fall within the intelligence community (for instance Spain, UK and Denmark). As a result, there are different databases at the NCSC, DefCERT and in the intelligence community – with the latter often unable to share reports that are classified secret or top secret.[43]

The concept of Public Private Partnership (PPP) is relatively well developed in the Netherlands, with much of the policy effort of the NSCS devoted to coordinating this. PPPs remain a cornerstone of cyber security policy, as neither the public or private sector are able to tackle the challenges of cyber security on their own. However, there are still divergent interests and important differences – such as who is going to pay for the added cyber security in national critical infrastructure – that need to be addressed.[44] The concept of Information Sharing and Analysis Centres (ISACs) is developing, and the NCSC plays a central coordinating role in these platforms. There are at least 14 sectoral ISACs, each dedicated to a specific sector such as banking and energy. Representatives of the major companies in these sectors meet regularly, on a voluntary basis, and exchange information on trends, threats, modi operandi, best practices and information on incidents. The ISACs are sector driven, with each setting its own agenda and determining policy, and the NCSC fulfilling only a facilitating role. While not formally a hub-and-spoke model, one of the two NCSC representatives in each ISAC generally fulfils the role of the secretariat, keeping the minutes. The other government participants in the ISACs are from the MIVD, AIVD and the Team High Tech Crime of the national police (THTC). Information is shared based on a traffic light protocol, which has largely allayed the private sector's concerns on liability, and the fear that any information shared could become subject to freedom of information laws.

2.2 Cyber within the Ministry of Defence

The Netherlands Armed Forces have three core tasks: 1. defending the Dutch national and alliance territories, including the Caribbean part of the Kingdom of the Netherlands; 2. protecting and promoting the international rule of law and stability; 3. providing military assistance to the civil authorities in the maintenance of law and order, emergency response and humanitarian assistance. The

[43] Senior officials at the MIVD and JSCU, interview.
[44] Clark et al., 'A Dutch Approach to Cybersecurity through Participation'; Carr, 'Public-Private Partnerships in National Cyber-Security Strategies'; Dunn-Cavelty and Suter, 'Public–private Partnerships Are No Silver Bullet'.

Ministry of Defence does not specifically acquire capabilities for this task, but civilian authorities can request any capacity that it does possess. There is for instance a catalogue of products and service, ranging from sandbags to trucks that can be requested by local or central authorities. This applies to emergencies as well as other situations, and there is a specific procedure that streamlines requests for the national deployment of Defence assets and clarifies questions of command and control. Cyber capacity, especially within DefCERT and Defence Cyber Command, has been integrated in the catalogue.[45]

Within the Ministry of Defence, DefCERT is responsible for the security of military networks and systems (monitoring and incident response), and has been fully operational since 2012. It is also tasked with ensuring that new systems and (weapons) platforms incorporate cyber security by design. DefCERT is part of the JIVC (Joint Informatievoorziening Commando), which operates under the Defence Materiel Organization.[46] The team currently consists of around 30 members, but will expand to 46 military personnel in the next two years. Most are involved in the monitoring of networks and incident response, while a small bureau focuses on the preventive element, tracking and reporting on relevant IT-developments and conducting risk assessments. A SOC to improve incident response is being created and will be operational in 2017, leaving more capacity for prevention. While the primary client is Defence, DefCERT can assist and support civilian authorities when requested to do so. Many requests are initially received informally, and subsequently redirected through official channels (the third national support task of Defence) so that DefCERT can comply and provide assistance. There is also a covenant for mutual support between DefCERT and the NCSC, and the former has twice assisted the latter in exceptional circumstances. The first concerned the DigiNotar crisis in 2011, when DefCERT personnel took over routine tasks from GovCERT operators, to allow them to focus on the crisis.[47] Secondly, in the preparations for the 2014 Nuclear Security Summit in The Hague, DefCERT conducted penetration testing on several government networks. This element of vulnerability testing is regularly done by DefCERT on military networks and systems, but the AIVD and MIVD are better equipped to conduct the more enhanced intruder assessments, so called red-teaming.[48]

DefCERT works with several national and international organizations and networks. It is connected to the NATO N-CERT/NCIRC, FIRST and other sharing platforms, and works with ENISA and the EDA. Its sharing partnerships are shaped by its institutional imbedding, and DefCERT's main partner is the German DefCERT that likewise is not in the intelligence sector. For the Royal Netherlands Army, and to a lesser extent the Air Force, this is a natural and convenient partnership, as they field many weapons systems that are also in German service. When for instance a Patriot anti-aircraft

[45] Senior official at Defence Cyber Command, interview.
[46] 'Defensie Computer Emergency Response Team', *Ministerie van Defensie*, accessed 12 May 2016, https://www.defensie.nl/onderwerpen/cyber-security/inhoud/defcert.
[47] Senior officials at the National Cyber Security Centre, Interview.
[48] Head of DefCERT, interview.

missile system in German service was hacked in 2015, there was much bilateral cooperation and DefCERT was kept informed on the investigation. In Belgium and the UK, the CERT falls within the intelligence community and sharing with DefCERT is thus limited, as is the information that is received from the MIVD and AIVD.[49] From a human resources perspective, DefCERT faces several challenges in recruiting and retaining qualified IT professionals. First, there is already stiff competition with the private sector, and cyber defence and monitoring is less exciting than penetrating and attacking foreign networks. High potentials and capable 'hackers' thus gravitate to where the action is, and this is not necessarily monitoring. Another problem is the lack of a cyber career path for military, with some military personnel having to return to their unit or service to fulfil compulsory positions to be able to continue with their regular career (in the infantry, artillery or other services). All organizations within the Ministry of Defence sector struggle with the acquisition of the necessary hard- and software. This can be such a lengthy and bureaucratic process that the purchased technology risks being outdated once it arrives.[50]

The Joint Sigint and Cyber Unit (JSCU), founded in 2013 and run by both the AIVD and MIVD, is tasked with signals interception (SIGINT) and obtaining intelligence through cyber operations. The law on the intelligence and security services determines when and under which circumstances they can operate and use special authorities to intercept and hack computers and networks, at home and abroad.[51] As part of the intelligence community - that must remain objective and free from political pressure – the MIVD and JSCU reside under the Secretary General of the Ministry of Defence (and for the JSCU also the Ministry of the Interior), and not the commander in chief. The cyber element within the JSCU has three missions: computer network defence, computer network investigation and computer network exploitation. In part due to cyber defence falling under the remit of the JIVC and DefCERT, but also as a result of a foreign intelligence agency's inherent tendency to focus on offence, computer network defence in the JSCU is less developed than investigation and exploitation.[52] The JSCU does contribute to the defence of several ministries (including the Ministry of Foreign Affairs), taking action against APTs from China, Russia, Iran and any other state sponsored threats.[53] The JSCU has equipment installed that monitors segments of Foreign Affairs' networks, but complete coverage remains elusive. Another problem is security awareness within the diplomatic sector, and the reluctance to deploy monitoring techniques that can be privacy intrusive, such as host based intrusion detection.

APTs are also a major concern for businesses in the Netherlands, and the JSCU has notified and assisted some companies after their networks had been severely compromised. The MIVD is

[49] Ibid.
[50] Ministerie van Defensie, 'Actualisering Defensie Cyber Strategie'.
[51] Wet op de Inlichtingen- en Veiligheidsdiensten 2002 (Wiv 2002).
[52] Senior officials at the MIVD and JSCU, interview.
[53] Algemene Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2015*.

responsible for ensuring that the Dutch Defence industrial base and companies providing or manufacturing military hard- and software conform to high cyber security standards. The MIVD, rather than the NCSC, supervises the Defence industry ISAC. This is the only ISAC that has legal structures and procedures in place to share highly classified signatures, modus operandi and tooling provided by the MIVD. The JSCU, and the mother organizations AIVD and MIVD, have extensive information sharing partnerships with their international partners in intelligence community and NATO. What is received, however, usually cannot be shared with national organizations like the NCSC or DefCERT. A report that is classified at the highest Top Secret COMINT level, cannot be 'downgraded' to the confidential or restricted level at which other government agencies operate.[54] The AIVD and MIVD try to release as much as possible to 'customers' outside the intelligence community through for example tearline reporting or briefings to selected officials (with the necessary security clearance) who need to deal with a specific threat.

Much cyber expertise will also be created within the Defence Cyber Command (DCC). This unit, which falls under direct responsibility of the Commander in Chief of the Dutch Armed Forces, was officially created in June 2015, and is predicted to be fully operational by late 2016.[55] Its mission is to develop and conduct offensive cyber operations, in support of military campaigns. The decision-making process and the ensuing mandate is therefore dependant on the laws and procedure that apply to the deployment of military force.[56] This is fundamentally different from the mandate of the intelligence services, and does not, for instance, permit intrusive cyber operations against potential adversaries in peacetime. To achieve its mission, the DCC is divided in three departments: the Technology Department, the Operations Department, and the Cyber Expertise Centre. The Technology Department will develop and deploy offensive cyber capabilities, all in accordance with the laws of war (*ius in bello*). The Operations Centre will train and field cyber advisors, who will support the commanders of operational units on the potential use of (offensive) cyber means, but equally on vulnerabilities of their own unit. These advisors will be the link between operations in the field and DCC in The Hague. Finally, the Expertise Centre will invest in knowledge and innovative capability within Defence. Since effective offensive cyber operations are without exception dependent on extensive groundwork provided by intelligence operations, the exact roles and responsibility of DCC vis à vis the JSCU still need to be worked out in much more detail.

2.3 Crisis management

The Ministry of Security and Justice is responsible for coordinating crisis decision making during large crises. Within the ministry, this role is assigned on the National Coordinator for Security and

[54] Senior officials at the MIVD and JSCU, interview.
[55] Ministerie van Defensie, 'Voortgangsrapportage over de uitvoering van de Defensie Cyber Strategie'.
[56] Arnold and Ducheine, 'Besluitvorming bij cyberoperaties'.

Counterterrorism (*NCTV*). Within the NCTV – placed next to the NCSC - there is a permanently manned National Crisis Centre (NCC), responsible for coordinating the crisis response and communication. Each ministry remains responsible for its own sector, and will activate a Departmental Coordination Centre (DCC) during a crisis. The coordination between ministries takes place in the inter-ministerial crisis board (*Interdepartementale Commissie Crisisbeheersing; ICCb*), a forum presided by the Director-General of the NCTV, with ministries represented by their Director Generals. This forum receives advice from a special Advisory team (*Adviesteam*), composed of experts from the NCC and other organizations. The same interdepartmental construction is mirrored one level higher, at the political level, where a Ministerial Board (*Ministeriële Commissie Crisisbeheersing; MCCb*) is presided by the prime-minister. The process of national decision-making in times of crisis is extensively proscribed in a handbook, but its underlying principle is that the structure should be simple and adapted to the specific circumstances.[57] The national crisis management structure, with slight adaptations, was for instance activated in July 2014, when flight MH-17 was shot down over Ukraine. A post-hoc evaluation concluded that the general crisis management structure functioned well, although cooperation with the specific first responders was slow to start.[58]

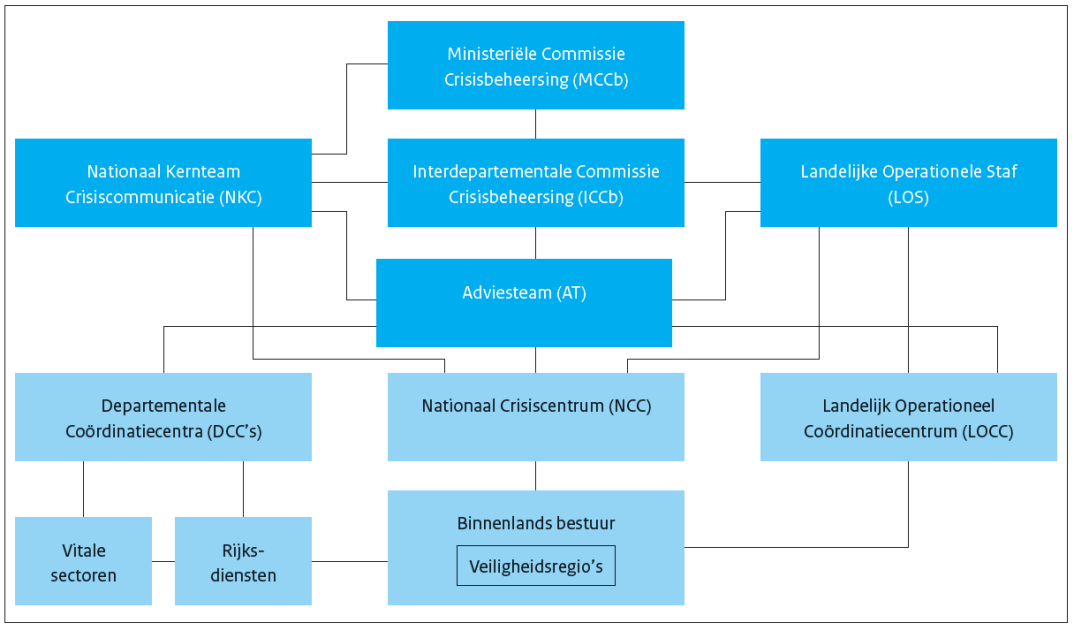


Figure 2.2 The Dutch cyber-conflict response structure59

While the generic crisis management structure remains applicable, for cyber or IT crises there are specific provisions, described in the National Crisis Plan ICT.[60] In such situations the NCSC is the coordinating hub, and the ministry of Economic Affairs has special powers to ensure cooperation of

[57] Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Nationaal handboek crisisbesluitvorming*.
[58] Torenvlied et al., *Evaluatie nationale crisisbeheersingsorganisatie vlucht MH17*.
[59] Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Nationaal handboek crisisbesluitvorming*, 37.
[60] Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Nationaal Crisisplan ICT*.

the ISPs and telecommunication providers. In the event of (potential) large-scale ICT disruptions, an ICT Response Board (IRB) can be activated.[61] This is a public-private forum that includes representatives from critical infrastructure sectors, telecommunications providers and ISPs, academic researchers, and CERT professionals. Its specific composition depends on the crisis. The chairman of the IRB is from the ministry of Economic Affairs while the NCSC provides the information coordinator. The IRB operates on the tactical level, and advises the strategic and political levels, such as ICCb/MCCb, in times of crisis.[62] The IRB is hosted by the NCSC and can also advise to the other private IRB parties such as critical infrastructure operators. This new structure had just been drafted when in September 2011 the DigiNotar crisis occurred. This crisis, which has been sufficiently analysed elsewhere, involved the compromise of the national certificate provider.[63] The national crisis structure was activated (including MCCb and ICCb), and an IRB provided advice to the decision-makers.[64] Much information and technical advice was provided by the (private) IT-security company Fox-IT, which was hired by DigiNotar once they suspected they had been hacked. Although the DigiNotar hack did not appear to result in a classic crisis with spectacular images of destruction, decision-makers recognized early on that trust in the Public Key Infrastructure was at stake, with potentially far reaching consequences. In post-hoc evaluations of the government's crisis response management, the reactive phase was largely regarded as well conducted, but the preventive phase was considered lacking. Prior to the hack there had been little security awareness at DigiNotar in particular and public ICT-organizations in general.[65]

The public-private network approach to crisis management is further embodied by the National Response Network (NRN), launched by the NCSC in 2014. This concerns a horizontal network of partners in different public and private sectors that can bundle capacity in the event of large cyber crises. The initial covenant was signed with five organizations: the information security service of the municipalities, the national tax authority, SURFNET (a collaborative organization for ICT in Dutch education and research) and DefCERT. The second pilot from 2015 onwards envisages that more organizations join: each new participant is expected to represent a large constituency, possess sufficient IT-capacity and be responsible for one or more vital sectors in the Netherlands. The Water Authorities (*Waterschappen*) have conducted a pilot to see if they can connect to the NRN.[66] As such, each partner has a unique capacity and specific experience to contribute the network. The tax authorities, for example, have much experience in countering DDoS attacks, while the Water authorities operate many Supervisory Control and Data Acquisition Systems (SCADA) systems. The

[61] Kaska, *National Cyber Security Organisation: The Netherlands*; Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Nationaal Crisisplan ICT*.
[62] Inspectie Veiligheid en Justitie, *Evaluatie rijkscrisisorganisatie tijdens DigiNotar-crisis*.
[63] See for instance Fox-IT, *Black Tulip Report*.
[64] Inspectie Veiligheid en Justitie, *Evaluatie rijkscrisisorganisatie tijdens DigiNotar-crisis*.
[65] Onderzoeksraad voor Veiligheid, *Het DigiNotarincident*.
[66] Taskforce Bestuur & Informatieveiligheid Dienstverlening, 'Voortgangsrapportage', 13.

goal is that in a time of crisis, this network can deploy the necessary response capacity and form a virtual human chain or bucket brigade to provide assistance where needed.[67] A problem that remains difficult to resolve is the varying response times, with public services generally reacting slower than the private sector.[68] Nonetheless, the NRN is another example of a public private partnership combined in a network approach, with the NCSC as a central, coordinating hub.

Dutch critical infrastructure has been the object of extensive analysis and policy in the past 15 years. Currently, there are 12 sectors identified as 'vital', each offering one or more products or services (31 in total), and each is coordinated by one or more government ministries.[69] Interestingly, Defence is not regarded as a separate vital sector, but one of the vital 'services' within the 'Security and Public Order' sector. After an initial analysis in 2005, followed by a second in 2009, the government decided in 2013 to recalibrate critical infrastructure (CI) protection. As many CI processes are interdependent and transcend different sectors, the analysis moved from a sectoral approach to charting the underlying processes that define vital services or products. This has led to new insights into risks, vulnerabilities and potential resilience of the concerned organizations, and several roadmaps to increase cyber security and resilience have been developed.[70] At the same time, to provide a better oversight of the CI landscape and enable a more effective prioritization in time of crisis, a new categorization of the importance of different services or products was made. To fall into either an *A* or *B* category, one of at least four impact criteria need to be met. For instance, the loss or serious disruption of an 'A grade' vital service could lead to 10.000 or more casualties or damages exceeding €50 billion, while for a 'B grade' vital service the figures are at least 1.000 afflicted persons or € 5 billion. While these figures are of course rough estimates and very much dependent on how a crisis evolves, they have helped identify the priority sectors and processes. The 'A grade' vital services are the provision of drinking water, the national transport of oil and gas, national electricity distribution, dykes and water defences, and the nuclear industry. Potentially difficult to calculate and incorporating a political element, the military still needs to be graded in an A or B category. Critical information infrastructure, such as the Amsterdam Internet exchange and also ISPs in general, have also not been categorized in the A/B priority yet.

As part of the 'recalibration' of critical infrastructure, in January 2016 a new cyber security bill was submitted to Parliament.[71] The national and international organizations that provide vital services must notify the NCSC if security breaches have occurred and/or they have suffered a loss of integrity of

[67] Jochem and Vos, 'Het Nationaal Response Netwerk: Een virtuele bucket line'.
[68] Head of DefCERT, interview.
[69] Nationaal Coördinator Terrorismebestrijding en Veiligheid, 'Resultaten herijking vitale infrastructuur'.; TK 2014-2015, 30 821, nr.23.
[70] Addae, Hebbink, and Hamelink, 'Herijking vitale infrastructuur'.
[71] *Wetsvoorstel Wet gegevensverwerking en meldplicht cyber security*, 21 January 2016. https://www.rijksoverheid.nl/documenten/brieven/2016/01/21/tk-voorstel-van-wet-inzake-wet-gegevensverwerking-en-meldplicht-cybersecurity

their vital ICT services. This only applies to breaches that could seriously disrupt the availability or integrity of ICT products or services vital to Dutch society, and for example DDoS attacks that only affect the accessibility of an online service do not need to be reported. The new law introduces specific guarantees to ensure the confidentiality and security of the data and information provided by the companies to the NCSC. This is to conform to privacy regulations, prevent reputation damage, or negatively impact on the competitive position of the companies involved. The bill determines when and how the NCSC can share the information with other parties, but the role of the NSCS in general remains advisory. It assesses the potential impact of the security or integrity breach, advises vital providers and warns third parties affected by the incident.[72] Enforcing compliance or imposing sanctions is not part of the NCSC's task, since this should be done by the sectoral inspectorates. As such, the NCSC's role is based on advising and informing others, very much in the centre of a public private hub and spoke model, and investing in trust building initiatives.

[72] *Nader rapport bij Wet gegevensverwerking en meldplicht cybersecurity*, *Memorie van Toelichting*, 21 January 2016. https://www.rijksoverheid.nl/documenten/kamerstukken/2016/01/21/tk-nader-rapport-inzake-wet-gegevensverwerking-en-meldplicht-cybersecurity

3 Denmark

Denmark was relatively late to the computer incident response scene, establishing a GovCERT early 2009. Recognizing that full packet inspection would be necessary for the GovCERT to function properly, the government first set about ensuring a strong legal mandate. At an early stage, privacy organizations were involved in the drafting process, and Parliament voted unanimously for the mandate and establishment of GovCERT. Initially the GovCERT was placed in the IT- and Telecommunication Agency within the Ministry of Science, Technology and Innovation, but late 2011 the new government decided that the country was too small for three separate public incident response centres (the Military CERT, Government CERT and a unit at the civilian security service PET). The Centre for Cyber Security (CFCS) was established in 2013, placing the Mil- and GovCERTs in the same department, but under different legal regulation. In 2014 the regulation was modified and milCERT and GovCERT are from January 2016 combined in one unit (CERT).[73] The government chose to embed the new centre within the *Forsvarets Efterretningstjeneste* (FE), or Danish Defence Intelligence Service (DDIS) by its English label. This is the country's foreign intelligence service, which falls under the remit of the Ministry of Defence.[74] The official name is Danish Defence Intelligence Service, Centre for Cybersecurity (DDIS/CFCS)

The reason for the transfer of all national computer incident response capacity to DDIS was a practical one. Defence already had the mil-CERT tasked with monitoring military networks and systems, and DDIS as the country's SIGINT service, already hosted the largest cyber talent pool in the country. The move was not wholly undisputed; within the military there were some proponents of setting up a separate cyber command, and some voices in civil society questioned whether placing GovCERT capacity in the intelligence community would lead to transparency and privacy issues. According to Danish CFCS officials, however, the current embedding is an efficient one for several reasons. Cyber defence is seen as intelligence based operations, based on the premise that high-level attackers or adversaries will always go for the weakest link or place in a network. Another advantage of being embedded in the intelligence community is that other forms of acquisition like HUMINT and SIGINT can be harnessed in investigations. As such, cyber defence (as well as cyber intelligence and cyber offence), are regarded as a 'team sport' whereby the combination of different sources is more than the

[73] Officials within the Danish Centre for Cybersecurity (CFCS), interviews Copenhagen.
[74] Järvinen, 'Danish Government Plans to Create a Center for Cybersecurity with Privacy-Invasive Powers'.

sum of their parts. While the government has officially decided to invest in offensive cyber capacity, there is currently debate on where to integrate this capacity in the DDIS/CFCS.[75]

3.1 Institutions and mandates

The CFCS is the Danish national ICT security authority. Its primary missions are to: a) contribute to protecting Denmark against cyber threats; b) assist in securing a solid and robust ICT critical infrastructure in Denmark and c) warn of, protect against, and counter cyber attacks.[76] Approximately 80 people work for the CFCS, divided into three departments: the Advisory and Telecommunications Department, which provides advice and assistance to the telephone companies and Internet Service Providers (ISPs); the Network Security Department, which is responsible for monitoring and incident response; and the Policy Department, which is responsible for threat assessments, strategies, and the future implementation of the EU's Network and Information Security (NIS) Directive. The initial mandate for the GovCERT has been significantly expanded for the CFSC by a new law[77] that allows the retention of traffic and packet data (that is not associated with a cybersecurity event for up to 13 months, [78] and what is shared with other cybersecurity services is kept indefinitely. As part of the intelligence community, the CFCS is exempted from Danish data protection and freedom of information laws.[79]

The CFSC is (on the basis of a mutual agreement) responsible for the monitoring and incident response of all government systems and networks, civilian as well as Defence. As most cyber attacks take place against civilian targets, it is here where most of the lessons are learned. The CFCS has the technical infrastructure (probes etc.) and the legal mandate for full packet inspection of all traffic in and to 18 of the 19 government ministries. The government ministries do have a responsibility for their own networks, and are expected to monitor, mitigate, and defend against low-level threats, such as so called garden variety malware that is less sophisticated and easier to detect. The ministries are in principle also expected to deal with simple DDoS attacks themselves. Apart from the central government, the CFCS monitors a number of private companies that provide services or infrastructure important to society, but their participation is on a voluntary basis. The separate DK-CERT handles security incidents on the National Research and Education Network (NREN) in Denmark.[80]

[75] O'Dwyer, 'Denmark To Develop Offensive Cyber Capability'.
[76] 'Organization Chart (DDIS)', *Danish Defence Intelligence Service*, 11 November 2015, https://fe-ddis.dk/eng/About-DDIS/Pages/Organization.aspx.
[77] Act No. 713, 25/06/2014.
[78] Ibid. §17.
[79] Järvinen, 'Danish Government Plans to Create a Center for Cybersecurity with Privacy-Invasive Powers'.
[80] Officials within the Danish Centre for Cybersecurity (CFCS), interviews Copenhagen.

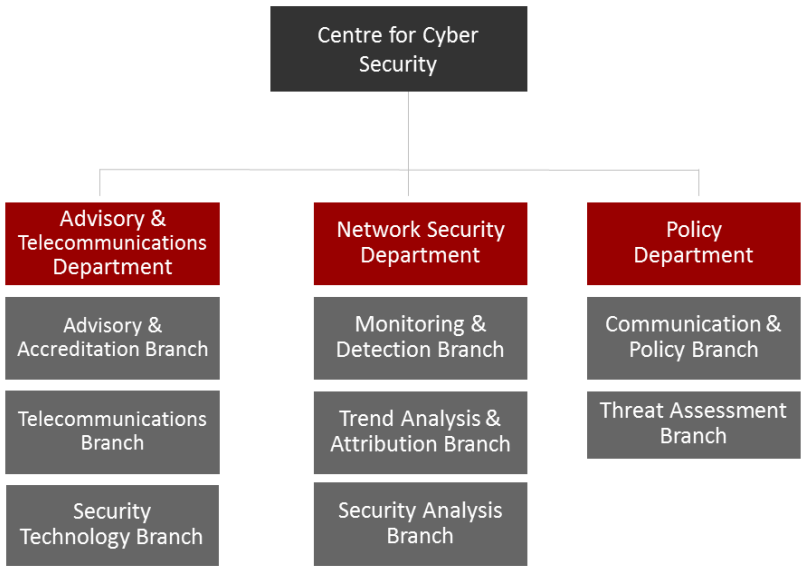


Figure 3.1 Organizational chart of the Danish Centre for Cyber Security. Source: CFCS, presentation given on 11 January 2016 (unpublished).

The CFCS is effectively the first responder to top-level cyber security threats in government networks and systems, being first to notice anomalies and discover intrusions. In its 2016 'Threat Assessment' report, the CFCS ascertains that espionage against Danish state institutions and companies constitutes *the most* serious cyber threat. This is mainly conducted by state and state-sponsored groups, and is continuing to increase significantly in its scope and sophistication. Some foreign states specifically target Danish authorities in an attempt to collect information on, for instance, Danish foreign and security policy. The CFCS also detects and prevents almost daily state-sponsored cyber espionage attempts against the Danish Ministry of Foreign Affairs.[81] In April 2012 the Ministry of Business and Growth was hacked, and the state-sponsored intruders attempted to map the Ministry's IT-infrastructure and obtain access to different accounts.[82] To halt the attack and expel the intruders, much of the ministry and its agencies was put offline and unable to use email for a short period of time. According to the CFCS, the threat of cyber espionage to the Danish private sector is equally estimated at *very high*. While the threat of cybercrime is also placed at *very high* (in comparison, cyber activism is put at *medium* and cyber terrorism at *low*), the CFCS estimates that criminal groups lack the organizational and technical skills that state-sponsored espionage groups have. Its capacity is focused on the top-level Advanced Persistent Threats (APTs), predominantly committed by other intelligence agencies.

[81] Centre for Cyber Security, 'Threat Assessment - The Cyber Threat against Denmark', 3–4.
[82] 'State-Sponsored Hackers Spied on Denmark'.

Denmark does not have a solid definition of what exactly constitutes (national) critical infrastructure. Like in most Western countries, however, critical infrastructure is predominantly in private hands, and companies are themselves responsible for the (cyber) security of their own platforms and systems. They have either developed a CSIRT or SOC capacity themselves, or source it from IT-security providers. Denmark supports the EU's aim of raising the baseline of cyber security in critical infrastructure, but considers cyber defence of critical national infrastructure a sovereign issue for member states. As such, Denmark does not support member states being compelled to share a comprehensive inventory and analysis of their own critical infrastructure with EU institutions and other member states, as this could also entail national security risks.[83] Denmark has an opt-out from EU-Defence cooperation, meaning that it does not participate in EU military operations or in the cooperation on development and acquisition of military capabilities within the EU framework. In NATO, however, Denmark has been part of a group of countries pushing to put cyber defence higher up the agenda of the alliance. The NATO Cyber Defence Development Plan has recently been approved by all member states and identifies minimum requirements for national information systems that are critical for carrying out NATO's core tasks.

On critical infrastructure, the DDIS works closely with the civilian intelligence and security service, PET. PET's Centre for Protective Security provides advice to the institutions and actors that are threatened, particularly those vulnerable or absolutely critical to Danish society. This segment includes, for example, Parliament and its members, the Royal Family, individuals under particular threat, ministries and agencies, public enterprises, foreign embassies in Denmark and Danish diplomatic missions abroad. PET also advises owners and operators of Denmark's critical national infrastructure in the areas of energy, transport, IT and telecommunications. Their advice incorporates physical security, personnel security and information security.[84] PET has its own 'Cyber Task Force' since July 2013, but relies on technical expertise from the DDIS/CFCS. In most cases the CFCS approaches a company together with a PET liaison to notify that it has been the victim of an APT.

When it concerns top-level state-sponsored espionage (or sabotage), in the 'incident response' phase, the CFCS is generally the first to arrive at the scene. Whether the lead was provided by (international) partner notification or the result of its own investigation, the CFCS informs the organization on the details of the cyber intrusion or attack. In liaison with the PET and police, the victim must decide whether to formally report the crime. Most companies are wary to do so, and for obvious reasons this also applies to the Ministry of Foreign Affairs that never reports cyber intrusions to the police. When a company is the victim and data from the telecommunication companies/ISPs is needed for the

[83] For an example of the Danish stance on the EU's role in protecting critical infrastructure, see a somewhat dated commission Green Paper with comments from the Danish government 'Danish Comments on EU CIP Programme'.

[84] 'The Centre for Protective Security', *Danish Security and Intelligence Service*, accessed 9 May 2016, https://www.pet.dk/English/Preventive%20security/The%20Centre%20for%20Protective%20Security.aspx.

investigation, a court order is required. This is requested by the company itself, and upon permission the CFCS can access any further data needed. A (confidential) written report is then sent to the company. All the malware data that has been collected during the investigation is added to the CFCS databases, contributing to its threat signature databases and malware repositories. This often also details the modus operandi of malicious actors. The data is subsequently used in future investigations, but the victim can determine whether content data is shared with other parties.[85]

The CFCS embedding in the intelligence community offers it important advantages when it comes to sharing information. In general, meta-data can be shared with similar cybersecurity centres and CERTs. IP addresses are considered unclassified information, but the context can be secret as it impacts directly on the privacy of those involved. To deal with this, the CFCS uses tear-line reports – a common practice in intelligence services, whereby the classified background of a conclusion or analysis is not shared when the recipients are not cleared. In this case only the (executive) summary is shared. Actual data content cannot be shared (except with the police). Even when legally permitted to share data, the CFCS determines on a case by case basis with whom it shares this information. A Danish official who has experience of both working outside the intelligence sector (the old GovCERT) and now in the CFCS as part of the DDIS, attests to the difference it makes for receiving information from others. He contends that he now receives much more information from international partners, especially the other intelligence services, than before. Previously he was unaware of what he was missing in terms of reports and classified information, and he can now observe how certain reports either arrive with a significant time delay at some partner cyber security centres outside intelligence, or often not at all. Sharing is based on a quid pro quo understanding, and if other centres have little to offer, there is little incentive for the CFCS to build a strong partnership with them.[86]

In December 2014 the Danish government presented a National Cyber and Information Security Strategy. The strategic goals, as stated by the document, are to improve the trust of citizens and businesses in the cybersecurity measures of the government and IT-sector, and to reinforce protection against cyber attacks of the key functions of society. Six focus areas are identified, and these have been translated to 27 specific initiatives that can be quantified. The government plans to update the strategy at the end of 2016.[87] The government also established the Agency of Digitization (under the remit of the Ministry of Finance) that is responsible for the digitization of the public sector.[88] The Danish police have also set up the National Cyber Crime Centre (NC3). The CFCS is nonetheless acknowledged as the national centre of expertise on cyber defence, but cooperates with the NC3 on

[85] Officials within the Danish Centre for Cybersecurity (CFCS), interviews Copenhagen.
[86] Ibid.
[87] Centre for Cyber Security, 'The Danish Cyber and Information Security Strategy'.
[88] "About the Agency for Digitisation," *The Agency for Digitisation*, accessed May 10, 2016, http://www.digst.dk/Servicemenu/English/About-the-Danish-Agency-for-Digitisation.

specific cases. There are also initiatives underway to more effectively pool resources and organize joint recruiting efforts for the police and intelligence sectors.

3.2 Crisis management

In Denmark, the Ministry of Defence has a strong role in national crisis management, in part due to historical reasons harking back to the Cold War. The Danish Emergency Management Agency (DEMA) is responsible for developing and strengthening preparedness for responding to major crises and accidents. The DEMA was founded in 1993 and integrated the State Fire service and the Civil Defence Agency. Its mission is to cushion the effects of accidents and disasters on society and to prevent harm to people, property and the environment.[89] In 2004 the DEMA was transferred from the Ministry of the Interior to the Ministry of Defence.[90] Within the ministry of Defence, the Office of Emergency Management oversees the DEMA as well as the Home Guard, a volunteer force of around 46.500 men and women that can be activated in war, national crises and even deployed abroad.[91] The extensive peace-time civil-military cooperation, which ensures collaboration and coordination across Denmark's defence agencies, Home Guard, police and emergency service units, is known as 'total defence' (*totalforsvar*).[92] It encompasses risk assessment, cross-sector readiness and the availability of military capacity to mitigate large crises and natural disasters. While international terrorism and the concept of hybrid warfare have confirmed the relevance and utility of 'total defence', institutional arrangements are still evolving. Previously, 'total defence' was led by the Danish Armed Forces, but the lead agency is currently the Danish Police, with the Danish Armed Forces standing by to contribute the means at their disposal, including military resources.[93]

Denmark has a national crisis management system that consists of several cross-sectoral crisis staff agencies that can be activated. They range from the Local Incident Command centres situated in the response area, to the Government Security Committee in Copenhagen, headed by the prime minister and consisting of the relevant ministers. The crisis management organization and its underlying principles are applied in a general and flexible way, to disasters, accidents or large-scale events such as summits. General principles for crisis response revolve around: a) sector responsibility, whereby departments or agencies that have a daily responsibility for a certain sector retain this during the crisis; b) similarity, whereby day-to-day procedures and responsibilities are applied to the largest extent possible; c) and subsidiarity, meaning that emergency management is handled at the lowest organizational level possible. In times of crisis, the National Operational Staff (NOST) is formed, a platform that coordinates the operation response and ensures that there is an overview of the

[89] 'About Us', *Danish Emergency Management Agency*, accessed 1 May 2016, http://brs.dk/eng/aboutus/Pages/aboutus.aspx.
[90] Britz, 'Translating EU Civil Protection in the Nordic States', 10.
[91] Danish Defence Commission, *Danish Defence - Global Engagement*.
[92] Matlary and Østerud, *Denationalisation of Defence*, 113.
[93] Danish Defence Commission, *Danish Defence - Global Engagement*.

situation.[94] Under the NOST, and mirroring its departmental composition, there is a Central Operational Communication Staff, responsible for providing information to the media and public. In each of Denmark's 12 police districts, a Local Operational Staff can also be established during a crisis to coordinate cross-sectoral cooperation. The DDIS is a permanent member of NOST and International Operational Staff (IOS).

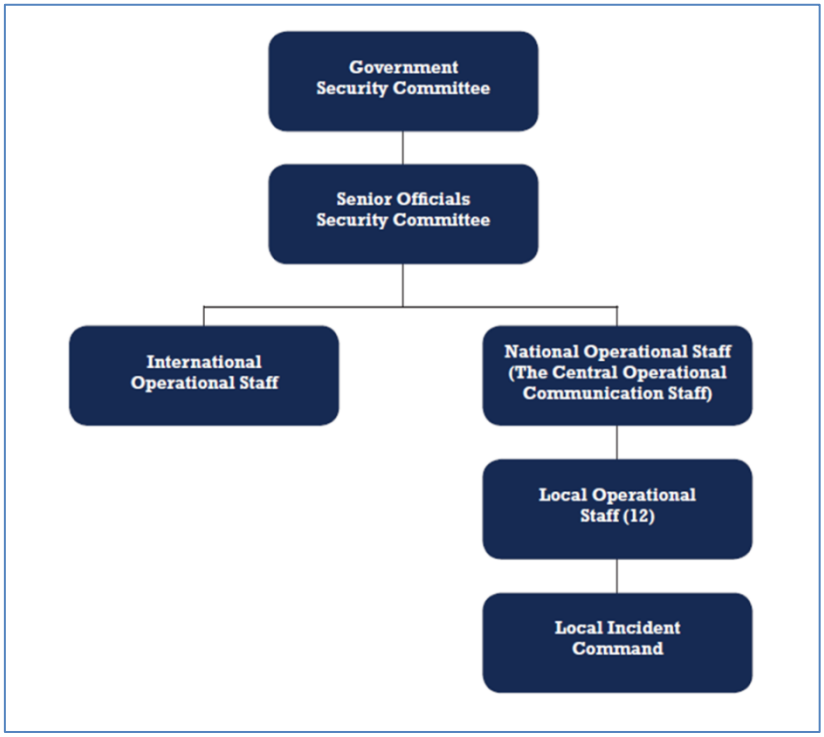


Figure 3.2 Organizational structure of Danish crisis management system95

Several large crises have tested and improved the national crisis management organization. In 2003 a power outage in the Swedish power grid caused a large blackout in Denmark also, affecting almost 5 million people for up to 6,5 hours. This led to traffic chaos in Copenhagen, trapped people in lifts and metro tunnels, and necessitated the temporary closure of the Øresund Bridge linking Denmark to Sweden. The NOST was activated, and this incident (and others) spurned Denmark to identify cross-sector risks and mitigate them. In 2005 and 2006 the Danish cartoon crisis occurred, after the newspaper Jyllands-Posten published twelve cartoons of the Muslim Prophet Mohamed. This triggered one of Denmark's most acute international political crises since the Second World War, causing demonstrations at home, threats against the cartoonist and newspaper, violent riots and the firebombing of several Danish Embassies abroad, and a boycott of Danish goods.[96] Here the International Operation Staff, coordinated by the Ministry of Foreign Affairs, took the lead in crisis management. Since 2005, risk assessments have formed a core element of planning for crisis

[94] Danish Emergency Management Agency, *Crisis Management in Denmark*.
[95] Ibid., 3.
[96] Wyman, 'Emergency Management in Denmark'.

situations, and annual vulnerability assessments reflect on past emergencies and propose initiatives for stronger prevention, planning, preparedness and response capacity.[97] As of yet, a cyber attack or cyber intrusion has not led to the activation of the crisis management organization.

The Ministry of Defence chairs the Crisis Management Group, a forum for planning, updating and practicing national crisis management scenarios. This forum focuses purely on prevention and preparation and is not activated during emergencies. The Crisis Management Group has several operational and regulatory tasks such as coordinating planning, prevention, education and training, and conducting exercises. There are biannual crisis management exercises, in which recently a coordinated and simultaneous cyber attack on the Danish health, electricity, and other sectors was simulated. Nearly a thousand officials were involved in this exercise which lasted two days.[98] The CFCS has its own internal crisis management structure that can be activated when necessary, and there are always team members on warning and availability notice. Rapid Reaction Teams can be formed and deployed at quick notice, and can be sent abroad as part of a military mission. Based on the initial description of the incident, the composition of the team is determined, including for instance specific malware or network experts. The team is subsequently sent to the organization suffering from a cyber crisis, and provides technical assistance. CFCS Rapid Reaction Teams have participated in the NATO exercise Locked Shields.

[97] Ibid.
[98] Officials within the Danish Centre for Cybersecurity (CFCS), interviews Copenhagen.

4 Estonia

Partly as a result of the famous cyber attacks in April/May 2007, Estonia has managed to become one of the leading authorities in cyber security and cyber defence.[99] Much has since been written on these attacks and their implications, but in essence they are considered more as a 'cyber riot' rather than an act of 'cyber war' by the Estonians themselves. At the time, however, the government found itself in a real crisis situation, with DDoS attacks swamping the websites of many organizations, including government ministries, Parliament, banks and media organizations. Not only did the highly connected society, with many government service offered online, seem at risk, but the crisis involved the large Russian minority (around a quarter of the population) and the assertive Russian neighbour. As a member of NATO, Estonia requested and received technical assistance; the only time as of yet that a member state has asked NATO for technical support in cyber defence. Nonetheless, at a political and strategic level it was made clear to the Estonian government that they should not even think of evoking NATO's article 4 (initiate consultation on a topic), let alone article 5 (collective defence).[100] After three weeks of incessant DDoS attacks and a near exhausted national crisis organization, the attacks suddenly stopped. The effect of the DDoS attacks were in part mitigated by temporarily disabling the top-level domain for Estonia (.ee), similar to an Internet kill switch for the country.[101] It is, however, important to note that that it was not an effective crisis management organization that found a solution to the crisis and ended it, but rather the perpetrators choosing to cease their attacks and therefore bringing the crisis to a close.[102]

There was ample evidence that Russian patriotic hackers were involved, but no forensic evidence proving that the Russian government was behind the attack.[103] Nonetheless, there are strong indications in other fields that still support this conclusion. According to Lauri Almann, then Permanent Secretary for the Estonian Ministry of Defence and a member of the Government Crisis Committee, Estonia was attacked by around 2 million bots hosted on servers in 175 jurisdictions, of which 174 cooperated with Estonia to take down the bots. Only one country did not: Russia. This was despite the existence of a detailed Russian-Estonian law enforcement agreement encouraging mutual legal assistance, signed in 1992 when relations between the two powers were still good.[104] This

[99] Mansfield-Devine, 'Estonia'.
[100] President Toomas Henrik Ilves, keynote address CyCon 2016
[101] 'Turning Around the 2007 Cyber Attack: Lessons from Estonia - E-Estonia', *E-Estonia*, 16 September 2013, https://e-estonia.com/turning-around-2007-cyber-attack-lessons-estonia/.
[102] Mansfield-Devine, 'Estonia'.
[103] For more details on how the Russian government was probably involved, see: Carey III, 'The International Community Must Hold Russia Accountable for Its Cyber Militias'.
[104] Mansfield-Devine, 'Estonia'.

agreement was used regularly by Estonian police to request Russian assistance and worked effectively for legal requests investigating for example violent crimes, but less so for politically sensitive incidents.[105] In this case Russia refused all help. As a result, only one perpetrator – from the Russian speaking community based in Estonia- has been tried and convicted for contributing to the attacks.

Estonia is famous for its advanced e-government scheme and connected society, boasting a high internet penetration and strong IT-sector that developed quickly after independence in 1991. Over 90% of the population uses the Estonian electronic ID-card, which enables many online services from tax reporting to voting.[106] Estonia has for instance carried out online voting for local and parliamentary elections eight times since 2008. Central to the e-government model is the X-road project, providing an infrastructure platform that allows interoperability and enables secure data exchange between different public and private organizations. More than 2000 services are offered by over 900 connected organizations, public registrars and databases, with over 500 million transactions taking place each year.[107] This is of course not only a vulnerable backbone, but also comprises a large attack surface that needs defending. The 'cyber riot' of 2007 has not eroded trust in e-government, and paradoxically led to even more use of the digital services.[108]

4.1 Institutions and mandates

Estonia's National Security Concept is the core strategic document that outlines the objectives and principle guidelines for the country's national security policy. This document is ratified by Parliament – the most recent version in 2010 - and provides a framework reference for other documents such as the National Defence Strategy and the Cyber Security Strategy.[109] After the 2007 cyber attacks, the ministry of Defence led an interagency effort to draft one of the world's first national cyber security strategies, to cover the timeframe 2008-2013. The strategy identified five objectives: a) the development and large-scale implementation of a system of security measures; b) increasing competence in cyber security; c) improvement of the legal framework for supporting cyber security; d) bolstering international cooperation; and e) raising awareness on cyber security. A new cyber security strategy was drafted for the period 2014-2017, and here the focus has been on consolidating the new structures that have been established.

In 2011 the coordinating role for national cyber security was transferred from the ministry of Defence to the ministry of Economic Affairs and Communication. This move was in part motivated by the necessity of setting and auditing digital security standards in the private sector, a task that did not fit

[105] Kadri Kaska, CCD COE, personal communications.
[106] Osula, *National Cyber Security Organisation: Estonia*.
[107] 'X-Road', *Cybernetica*, accessed 12 May 2016, https://cyber.ee/en/e-government/x-road/.
[108] 'Turning Around the 2007 Cyber Attack: Lessons from Estonia - E-Estonia', *E-Estonia*, 16 September 2013, https://e-estonia.com/turning-around-2007-cyber-attack-lessons-estonia/.
[109] 'National Security Concept of Estonia'.

well in the military's mandate. The importance of civilian leadership is emphasized in the new national cyber security strategy:

> To ensure the ability to provide national defence in cyberspace, the state's civilian and military resources must be able to be integrated into a functioning whole under the direction of civilian authorities as well as being interoperable with the capabilities of international partners.[110]

At the same time as the transfer to civilian leadership, the Estonian Information Systems Authority (*Riigi Infosüsteemi Amet*; RIA) was created as the central cyber security competence and coordination centre. This was embedded in the ministry of Economic Affairs and Communications (MEAC), as the new authority for coordinating national cyber security policy. The RIA is responsible for the development and administration of state information systems, as well as drafting related policies and strategies, coordinating the implementation of security standards, handling security incidents either reported or occurred on Estonian networks.[111] The MEAC thus drafted the new cyber security strategy for 2014-2017, alongside the ministries of Interior and Defence. The strategic objectives as related to critical information infrastructure protection (CIIP)were drafted by RIA. The RIA not only has a national coordinating role, but also supervises the implementation of security standards and policies, and has a mandate to conduct extrajudicial proceedings and impose fines when companies and organizations fail to conform to the rules.[112] Within the RIA, a new Cyber Security Service comprises three organizational units: the CERT-EE, a risk management Department (including CIIP), and a Research and Development Department.

The CERT-EE, combining the national and GovCERT functions, was formed in 2006 and is the primary entity responsible for managing security incidents in .ee networks.[113] The CERT services are divided into a proactive role, that consists of improving awareness, giving advice on managing cyber risks, collecting and providing information on specific threats and developments, and coordinating information sharing. Security assessments in the CII sector are also conducted, and RIA supervises the implementation of cyber security regulation. The reactive task, which was put to the test one year after the CERT's establishment, includes triage and incident response. The CERT will host the Virtual Situation Room, a communications platform for crisis prevention that facilitates cooperation between service providers and government agencies. This platform, currently under development, combines different tools and datasets to analyse and visualize developments in an easy to understand form.[114]

[110] 'Cyber Security Strategy 2014-2017', 6.
[111] Osula, *National Cyber Security Organisation: Estonia*.
[112] Ibid., 6.
[113] Kouremetis, 'An Analysis of Estonia's Cyber Security Strategy, Policy and Capabilities'.
[114] 'Virtual Situation Room', *Information System Authority Republic of Estonia*, accessed 12 May 2016, https://www.ria.ee/en/vsr.html.

When serious security incidents occur in the networks of state entities, they are obliged by law to immediately notify the CERT-EE, and they must also submit quarterly cyber security reports. [115]

Whereas the CERT-EE has a strong emphasis on the operational level, the Cyber Security Service has a predominant strategic focus. The department was established in 2009, and is tasked with ensuring that Estonia's information and communication systems function at all time, including during crises. Its mandate therefore covers the whole range of preparedness, prevention, incident response, up to resilience, and the department conducts many different activities to this end. They include mapping information infrastructure and its dependencies and vulnerabilities, conducting risk analyses and creating and maintaining a supervisory system for the implementation of security measures.[116] On the national level, this means focusing on protection of the public and private sector information systems that ensure the functioning of vital services. The Emergency Act has identified 43 vital services in Estonia that are critical to the functioning of society, and these are provided by over 140 public and private sector organizations.[117]

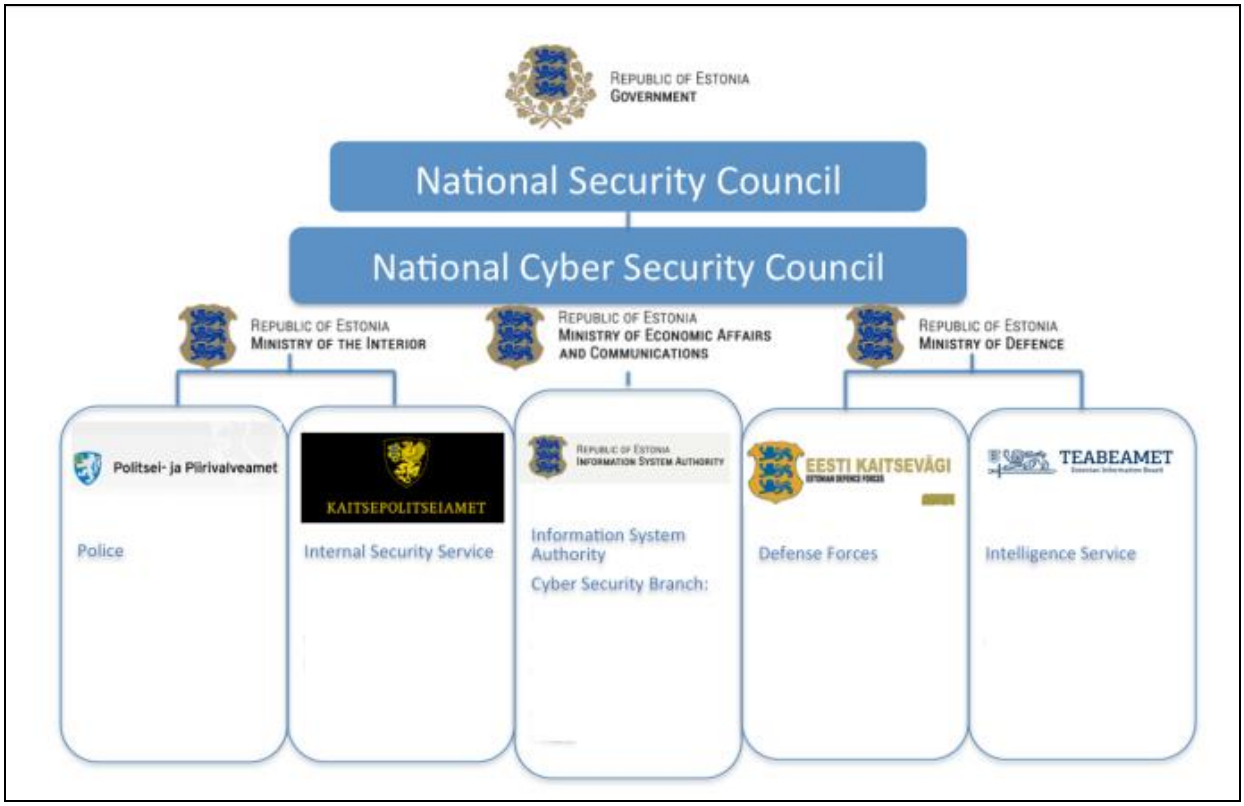


Figure 4.1 Cyber Security Framework in Estonia. Source: Luht, 'Cyber Emergency Preparedness and Response: Estonian Approach', presentation at CyCon 2016 (unpublished).

[115] Osula, *National Cyber Security Organisation: Estonia*.
[116] Kouremetis, 'An Analysis of Estonia's Cyber Security Strategy, Policy and Capabilities'.
[117] 'Critical Information Infrastructure Protection CIIP', *Information System Authority Republic of Estonia*, accessed 12 May 2016, https://www.ria.ee/en/ciip.html.

The second Cyber Security Strategy led to a large consolidation of cyber capacity within the police and Border Guard in 2012, combining them in one department. The units within the regions (prefectures) that dealt with cybercrime and digital evidence management procedures were also consolidated.[118] Under the remit of the ministry of Interior, there is another unit with cyber capacity that conducts investigations into top-level threats. Estonia's combined internal security and foreign intelligence service (*Kaitsepolitseiamet, or Kapo)* is tasked with identifying cyber attacks that are initiated by foreign states and may threaten national security.[119] From open sources the exact relationship with the CERT-EE and cyber units within Defence is unclear.

The ministry of Defence plays an important role in coordinating national cyber defence. The Strategic Communications Centre is responsible for the security and continuity of the ministry's networks and communications infrastructures, and research and development, which includes maintaining and developing the cyber range.[120] This cyber range has been used by its own cyber defence forces, those of allied states and the NATO alliance for cyber defence training and exercises. What was originally an exercise supported by Estonia and Sweden (Baltic Shields) became Locked Shields in 2012, and is now the biggest and most advanced annual international 'live-fire' cyber defence exercise in the world. In April 2016, for example, Blue Teams representing 19 nations and the NATO Computer Incident Response Capability (NCIRC) participated in the exercise, all joining the exercise online, while stationed in their home countries. The scenarios typically train cyber defence, with Blue Teams tasked to maintain the networks and services of a fictional country, and react to Red Teams trying to sabotage the system. The exercises combine the technical handling and reporting of incidents, the solving of forensic challenges as well as responding to legal, media and scenario injects.[121]

International cooperation and NATO have been cornerstones for Estonian security policy. Partly as a result of the 2007 cyber attacks, Estonia has become a successful leader in cyber defence initiatives. Tallinn hosts the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE). Estonia had suggested to launch this centre as early as 2003, and although the U.S. was enthusiastic, no other country was initially interested with much attention focused on countering IEDs and the operations in Afghanistan and Iraq at that time.[122] After the 2007 cyber attacks, the initiative gained momentum, with initially seven countries contributing. The centre conducts cyber-security research in the field of governance, policy, and strategy, but also works on tactical and operational concepts. The CCD COE hosts and organizes many different workshops, trainings and exercises, forming the most important hub of cyber expertise in NATO. In 2016, the number of participating NATO countries is expected to increase from 18 to 20, and the concept of its large annual international Cyber Conflict Conference

[118] 'Cyber Security Strategy 2014-2017'.
[119] 'Annual Review 2015 Estonian Internal Security Service'.
[120] Osula, *National Cyber Security Organisation: Estonia*.
[121] 'Locked Shields 2016', *CCDCOE*, 15 April 2016, https://www.ccdcoe.org/locked-shields-2016.
[122] Jackson, 'Estonian Cyber Policy After the 2007 Attacks'.

(CyCon) will be replicated by the U.S. army. This is not to say that the cyber attacks of 2007 have awoken NATO to cyber defence; the alliance has its own networks to defend and has been preparing to do so since the early-2000's. Other member states, however, have been less keen on investing in cyber, and Estonia plays an active role within NATO in keeping the issue high on the political agenda and sharing knowledge and expertise.

The Cyber Defence Unit of the Estonian Defence League (*Kaitseliit*) is a concept that has attracted widespread international interest as an innovative model of using volunteers in cyber defence.[123] The Estonian Defence League has a long history as the country's volunteer fighting force (dating from 1918), and was restored after Estonia's independence in 1991. In the aftermath of the 2007 cyber attacks, a sub-unit of computing and IT-specialists was set up within this force. This Cyber Defence Unit has several aims, including promoting general awareness and strengthening the professional cyber defence skills of its members, to be able to provide support during crises. Specialists that want to join need to navigate a strict application process and pass background checks. Referees are required to recommend the candidate, and all this implies that black-hat hackers need not apply. To promote the concept abroad, the Estonian ministry of Defence requested the NATO CCD COE to conduct a study of the Cyber Defence Unit, focusing on the legal, organizational, and policy questions. The resulting 45-page report, published in 2013, provides a valuable insight into this unique volunteer force of cyber professionals, but also lays bare some specific elements that limit the applicability of the model abroad. As such, it is described as an emerging capability that is not yet a final product, but is in the process of evolving in a bottom-up fashion to become a valuable cyber defence force.[124]

The principle of voluntary participation and self-initiative lie at the heart of the Cyber Defence Unit, and form its strength and weakness at the same time. The volunteer component has nurtured an organic growth, with many motivated and capable volunteers enriching the organization. As a collective network, they increase awareness in the general IT-sector, and there has been increasing interest to join after Russia's annexation of Crimea.[125] At the same time these volunteers cannot be obliged to participate in any specific activities of the organization, and they receive no salary for their engagement in the unit's activities (although remuneration of direct costs is possible). The principle of voluntary participation poses a potential problem during IT-crises, as unlike reservists, members cannot be called up to serve. As Estonia has mandatory national service, many members are reservists anyway.[126] During crises it is difficult to rely on the Cyber Defence unit, with many volunteers working on their day jobs in the private sector, and potentially already involved in the first line of the crisis. Nonetheless, the concept of the unit as a network of volunteers operating on the basis of trust

[123] Cardash, Cilluffo, and Ottis, 'Estonia's Cyber Defence League'.
[124] Kaska, Osula, and Stinissen, *The Cyber Defence Unit of the Estonian Defence League*.
[125] Padar, 'The Estonian Cyber Defence Unit'.
[126] Reservists can only be activated in case of a military threat, and not a lower level ICT-crisis, but participation in the Cyber Defense Unit can help appropriately assign ICT reservists.

does seem to transcend the organizational boundaries of Defence, CERT-EE and Kapo, and build a bridge between the public and private sector. All members have clearances, and the informal culture and network organization facilitates a fast exchange of information, allowing efficient cooperation between different agencies.[127]

4.2 Crisis Management

Generic crisis management is governed by two main legal frameworks: the Emergency Act (2009) and the State of Emergency Act (1996).[128] Each ministry is responsible for its own domain and dossiers, and the ministry of Interior is in charge of the National Crisis Management Committee, acting as the central coordinating authority in emergencies. In addition, the ministry of Interior is responsible for civil protection, internal security, rescue operations, and citizenship and immigration. The ministry of Economic Affairs and Communication is responsible for ensuring the continuity of the country's communication and IT- networks – the critical information infrastructure. The Emergency Act provides the structures and procedures for government organizations in times of emergency, but also stipulates the legal qualifications for emergency preparation and response, and what vital services must be guaranteed. An 'emergency situation' can be declared by the government if extraordinary security measures are warranted. In exceptional circumstances a 'state of emergency' allows the restrictions of specific individual rights and freedoms. The Prime Minister is the chief authority during a state of emergency, and only the President or government can declare it in the event of a threat which undermines the constitutional order. The 'state of emergency' has never been declared since the adoption of the constitution, while in recent years, an 'emergency situation' has been declared during several natural disasters, and also for the 2007 cyber attacks.[129]

According to RIA's 2015 Annual report, several large-scale cyber exercises were organized in 2015. These included the national cyber exercise Cyber Hedgehog, crisis management exercise CONEX, and participation in NATO's Cyber Coalition and the EU's Cyber Europe exercise. The CONEX table-top exercise was organized at a strategic level, and involved the minister of Economic Affairs who had to respond to a large scale cyber attack on the nation's ID-card infrastructure and other vital infrastructure. Both the CONEX and Cyber Hedgehog exercise revealed the inadequacy of the current legal framework. As a result of the lessons identified, RIA underlined the need for a separate law to increase legal clarity and define responsibilities at a national level. The ministry of Interior has subsequently drafted a proposal for a new Emergency Act to clarify the domain of the nation's vital services. As these services are regulated by sector specific acts, various separate acts will also need to be established or updated. This process coincides with the EU's NIS directive. This defines the

[127] Ibid.
[128] Osula, *National Cyber Security Organisation: Estonia*.
[129] Hellenberg and Visuri, 'Analysis of Civil Security Systems in Europe Country Study Estonia'.

provision of vital services in member states and the cooperation of CERTs during incident response, and needs to be implemented in national law in the next two years. Rather than amending a series of sector specific laws, the RIA annual report recognizes that developing a new comprehensive legal framework, integrating the NIS directive together with the necessary updates to existing law, would be the preferred solution.[130] The jury is still out whether this one comprehensive and compact law can be drafted.

[130] '2015 Annual Report of the Estonian Information System Authority's Cyber Security Branch', 12–13.

5 The Czech Republic

The first policy initiatives on Czech national cyber security originated from the Ministry of Interior, which is responsible for the fight against cyber crime. In 2010, a memorandum established the National Cyber Security Incident Response Team within the CZ.NIC, a legal association of the country's largest ISPs. This later became the National CERT. A year later, the Strategy for Cyber Security 2011-2015 and the accompanying action plan were launched. This provided the first blueprint for cyber security, although many of the recommendations were formulated in a generic fashion and were inspired by EU documents. In October 2011 the Czech government passed resolution 781, which gave the National Security Authority (NSA) overall responsibility for national cyber security. The same resolution established the National Cyber Security Centre (NCSC), subordinate to the NSA and home of the government CERT.[131] The NSA, which is a separate government agency on the same level as a ministry (but without representation in the cabinet), has since coordinated national cyber security policy. The NSA drafted a new National Cyber Security Strategy for the period 2015-2020, and will work on and monitor the implementation of the Action Plan that is part of the strategy.[132]

Two elements stand out in current Czech cyber policy. First, the cyber attacks on several Czech servers and websites in March 2013 have formed a frame of reference and a wake-up call for national cyber security. Over the course of several days, Distributed Denial of Service (DDoS) attacks caused several major news services, search engines, the websites of major banks and the Prague stock exchange to become unavailable. While several services went offline, no data was stolen or compromised and experts estimated that the disruption caused was limited. Attribution proved to be difficult, and the trail ended when a Russian telecommunications network, from which several involved botnets originated, stated it could not cooperate with the investigation and had no data to share. Not everyone is convinced that the Russian government was involved, but there is consensus within the Czech security establishment that the attack was a testing exercise for a larger attack yet to come.[133] This notion of the Czech IT-infrastructure as a test bed for an attack on countries with greater strategic importance but using similar technologies and procedures, is identified as an important challenge (at the top of the list) in the current National Cyber Security Strategy.[134] The second reoccurring theme is the Czech ambition to play a leading role in the cyber security field within its own region and in Europe in general. To this extent the Czech Republic has organized several events

[131] Minárik, *National Cyber Security Organisation: Czech Republic*.
[132] National Cyber Security Centre, *Czech NCSS 2015-2020*; National Cyber Security Centre, *Action Plan for the NCSS 2015-2020*.
[133] Kostyuk, 'International and Domestic Challenges to Comprehensive National Cybersecurity'.
[134] National Cyber Security Centre, *Czech NCSS 2015-2020*, 11.

to put cyber on the agenda in the Visegrad Group (Poland, Hungary, Slovakia and the Czech Republic) and plays an active role on cyber issues in the EU and NATO. As for the grander European ambitions, other small EU and NATO countries, like Estonia, are also competing to shine as leaders in cyber innovation and expertise.[135]

5.1 Institutions and mandates

The decision to embed the National Cyber Security Centre within the NSA - and not the ministry of Interior or Defence - was probably made for practical as well as personal reasons. The director of the NSA has an engineering background and has always had a strong interest in cyber security, personally driving policy on the topic.[136] His tenure as director of the NSA since 2006, combined with his authoritative status within government circles, made the NSA a logical agency to coordinate national cyber policy. The NSA is responsible for personnel and facility security clearance procedures, issuing certificates and clearances, certifying cryptographic devices, determining and auditing the rules of national classification procedures, and approving the release of classified information internationally.[137] According to Czech officials, it was a conscious decision not to embed the NSA in the intelligence community, as this would risk complicating the sharing of information. This would go both ways, with classification issues impeding public to private sharing of information, but the fear was also that the private sector would be more reluctant to share with the intelligence service, for historical as well as contemporary reasons.[138]

Within the NSA, the National Cyber Security Centre (NCSC) operates the GovCERT function. This entails managing the cooperation with CSIRTs, both national and international, preparing security standards for various entities and supporting cyber security awareness programs, and stimulating education and research and development.[139] Based in Brno, the Czech Republic's second largest city, the GovCERT collects reports of cyber incidents, analyses them and provides assistance. Notwithstanding several probes the GovCERT has deployed in the networks of subjects which expressed their direct consent, monitoring networks is principally the responsibility of the ministries, agencies and companies themselves. Its main constituents are the public sector (ministries and agencies) and the nation's critical infrastructure (CI), which is in private or public hands. There is no widespread deep packet inspection (DPI), and while organizations can choose to conduct DPI on their own networks, the specific criteria that have to be met for this are still under deliberation. Underlying

[135] Mad'ar, *Aiming for the Stars*.
[136] The deputy directors and others from the NSA's leadership also had a significant influence in this regard. Officials at the National Security Authority, personal communications.
[137] 'National Security Authority', *NBU*, accessed 25 May 2016, https://www.nbu.cz/en/.
[138] Officials at the National Security Authority, personal communications.
[139] Minárik, *National Cyber Security Organisation: Czech Republic*.

the relationship with these entities is the subsidiarity principle, whereby the organization in question understands its own networks best, and has the first responsibility for monitoring them.[140]

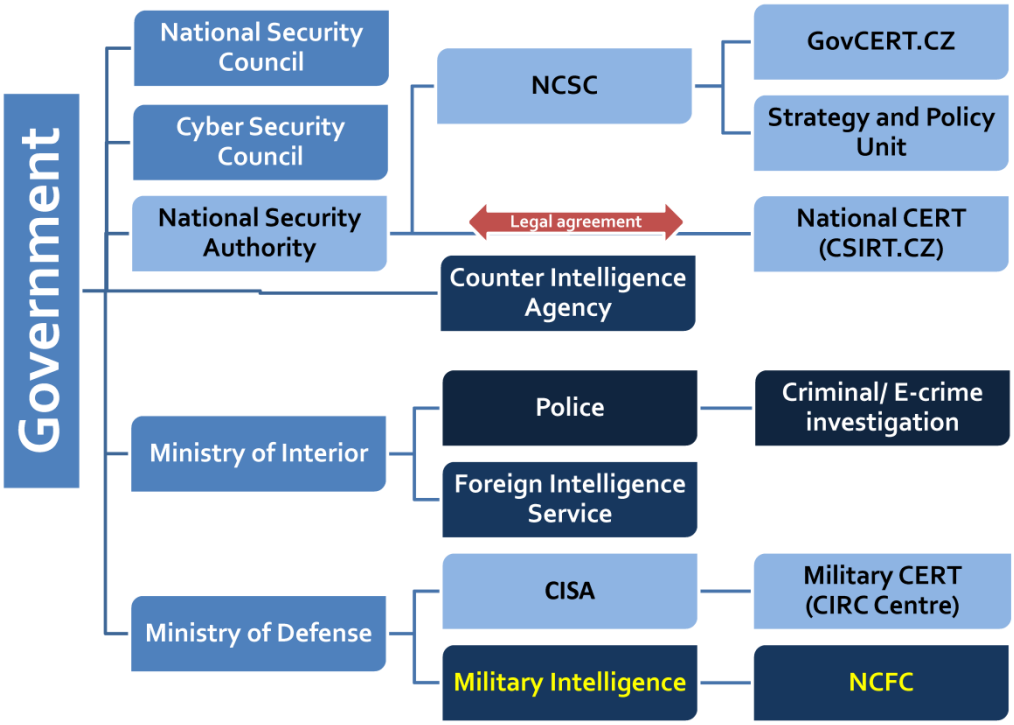


Figure 5.1 Czech cyber security organization.[141]

Parallel to running the public sector GovCERT, the NSA has contracted the private association CZ.NIC to operate a National CERT (CSIRT.CZ) for the private sector.[142] This covers the main ISPs and other private parties, although there is some overlap with critical (information) infrastructure falling under the remit of GovCERT. The distinction is that CII and IIS fall under CSIRT.CZ in day-to-day business, while they become GovCERT's constituency in the state of cyber emergency. As a public body, GovCERT can only do what the law prescribes, while the national CSIRT.CZ can do anything that is not illegal. Their information sharing circles are equally divergent, although both CERTs mainly get information from their respective constituencies. The major distinction is that GovCERT can cooperate and share information with international organizations (i.e. EU (ENISA) and NATO (NCIRC)), while CSIRT.CZ has strong established links with the private sector for this purpose. Both CERTs are members of FIRST- network of CERTs. Nonetheless, as the CZ.NIC is one of the first NGOs that deals with reported incidents in times of crisis, they have accumulated high

[140] Officials at the National Security Authority, interview.
[141] Officials at the National Security Authority, personal communications.
[142] 'About Us', *CSIRT.CZ*, accessed 2 May 2016, https://www.csirt.cz/page/882/about-us/.

levels of expertise. Their experts are therefore established as the NSA's main partners in crisis management, and they are often the first to go to the scene.[143]

The military has its own Computer Incident Response Capability (CIRC) that falls under the remit of the Communications and Information Systems Agency (CISA). The CISA is part of the Support Division of the General Staff of the Czech Armed Forces, and is responsible for *command & control* and *communications* systems of the ministry of Defence. Tasked also with ensuring cyber security in the military domain, the CISA has a framework memorandum with the NSA as the civilian national cyber security authority. The mission of the CIRC is the "proactive identification of security threats and incidents, their analysis and subsequent reporting of events and solutions to relevant partners."[144] The CIRC participates in both national and international cyber defence exercises, cooperates with NATO's NCIRC and participates in the malware Information Sharing Platform.[145]

In 2016 a national Cyber Forces Centre was established in Military Intelligence, with the aim of being fully operational by 2020. In the 'Long Term Perspective for Defence 2030', the government plans an intensive build-up of cyber defence capabilities (as part of Cyber Defence and Information Assurance activities) in the form of passive, preventive and reactive measures. Military Intelligence and the Armed Forces will develop cyber warfare capabilities while ensuring the principle of "jointness".[146] The term 'cyber offence' is not mentioned, nor is 'active defence' clearly defined. Presumably this encompasses penetrating an adversary's networks to gain advance warning of attacks (or assist in attribution if this fails).

When comparing the allocated budgets, it becomes clearer where significant cyber capacity will reside in the public sector. The civilian NCSC will receive 115 million CZK per year (around € 4,25 million), while the budget for cyber defence in the military is planned at 500 million CZK a year (€ 18,5 million).[147] This cyber capacity, when it comes online, could potentially provide a significant boost to national incident response.

5.2 Crisis Management

In general crisis situations, the prime minister can activate the Central Crisis Staff, the government's primary forum for managing emergencies. Depending on the type of crisis, it is chaired by either the minister of the Interior or the minister of Defence. Then Central Crisis Staff can declare a 'state of emergency', advises the National Security Council or government ministers directly, and is responsible for coordinating, monitoring, and evaluating the measures taken during the crisis. It is fed

[143] Officials at the National Security Authority, interview.
[144] Minárik, *National Cyber Security Organisation: Czech Republic*, 10.
[145] Minárik, *National Cyber Security Organisation: Czech Republic*.
[146] Ministry of Defence of the Czech Republic, *Long Term Defence Perspective 2030*.
[147] Minárik, *National Cyber Security Organisation: Czech Republic*, 12.

information by the Regional Crisis Staff (headed by the Head of Region) and the Local Crisis Staff (headed by the mayor). These units incorporate the heads of the fire and police services, and are the first responders to the crisis in their area of responsibility. The national crisis structure has previously been activated during for example the floods in August 2002, and the Prague NATO summit in November 2002.[148] However, this structure was not activated during the 2013 DDoS attacks, as they did not reach the threshold to be regarded a (general) crisis.[149]

In 2015, the Czech Republic passed the Cyber Security Act, a comprehensive legal framework for identifying national critical infrastructure and setting out responsibilities for the organizations involved. One of the main objectives of the legislation is to implement security standards for the information systems of public authorities as well as critical infrastructure. First, the government compiled a list of 45 elements of critical infrastructure operated by the public sector, in May 2015. Since then, the NSA has continued to determine CII elements in both the public and private sector, including electricity, gas, and railway companies, air traffic management, and ISPs.[150] As of May 2016, 48 elements in the public sector have been identified as CII, versus 50 in the private sector.[151] There is also a third category, of information systems that are not deemed critical for society, but are vital for public administration. These are classified 'important information systems' (IIS), and subject the operators to about 60% of the obligations imposed by the Act on Cyber Security. The standards that should be followed are based on the ISO/IEC 27000 series and provide a detailed description of the preventive security measures required. These include comprehensive management, organizational and security procedures, tailored to specific categories of organizations. At the same time the Cyber Security Act also specifies the procedures for reporting cyber incidents to either the GovCERT or the CSIRT.CZ. The NSA plays an important role in enforcing these security standards, and conducts periodical compliance audits of all public administration bodies as well as private elements of the critical national infrastructure.[152] The NSA has the authority to impose fines if organizations have not followed the regulations.

A unique element of the Cyber Security Act is the ability to declare a 'state of cyber emergency'. This can be declared by the NSA if the national interest is seriously endangered by a large scale threat to information security or to the security of electronic communications services. The policy unit and GovCERT within the NCSC advise the director of the NSA, who must inform the prime minister after taking the decision. The state of cyber emergency has a media and political function, but also a technical one. It permits the director of the NSA to order ISPs or entities operating national CII to take specific measures to mitigate the crisis. The state of cyber emergency is initially established for a

[148] Kosek, 'Crisis Management in the Czech Republic'.
[149] Officials at the National Security Authority, personal communications.
[150] Minárik, *National Cyber Security Organisation: Czech Republic*.
[151] Kadlecova, 'Presentation Cyber in the National Crisis Management System: The Czech Republic'.
[152] Andrš, 'Czech Cyber Security: Finally ahead of Europe?'

period of 7 days, but can be prolonged to up to 30 days. Once the threat has been countered or the crisis managed, it is the director of the NSA who can lift the state of cyber emergency. If the cyber crisis exceeds the legal timeframe of 30 days, a general state of emergency can be declared. The state of cyber emergency has never been declared yet, but the concept was tested in NATO's CMX 2016 exercise. While the concept held up well, lessons learned included the need for expanding the group of stakeholders involved in crisis decision-making, and the importance of contextualizing cyber information for the generic crisis management process.[153]

As an active member and participant in the NATO alliance, as well as in the EU's foreign and security policy, the Czech government is involved in many international initiatives. In the field of crisis management, the annual CCDCOE exercise 'Locked Shield' has been a good way to train incident and crisis response. The Czech team – made up of GovCERT/NCSC and strengthened by the military CIRC[154] – has participated every time, frequently winning prizes in multiple categories for their role in the exercise. This has helped the military build up a certain expertise that is unique in Czech cyber landscape, and would make a request for their assistance in a crisis situation a logical reaction. Inspired by Locked Shields, the NCSC also organizes a national exercise, 'Cyber Czech', in cooperation with Masaryk University in Brno. The focus is on defending national critical information infrastructure, and participants are put into the role of CSIRT or Rapid Reaction Teams sent into unknown networks to recover compromised networks. Beside the main technical component, there are also a policy and media challenges involved.[155]

[153] Kadlecova, 'Presentation Cyber in the National Crisis Management System: The Czech Republic'.
[154] Officials at the National Security Authority, personal communications.
[155] Vykopal and Mokoš, 'Czech Cyber Defence Exercise: Lessons Learned'.

6 Analysis

The different institutional landscapes studied in this report are all products of a specific political history and culture. Each country has unique political traits and traditions. In one country, for instance, the military traditionally plays a strong and respected role, while in another, mid twentieth century history might have led to a distrust of intelligence agencies. As 'cyber' becomes ubiquitous, it is only logical that the underlying political landscape is reflected in the institutions where cyber security capacity has been built up.[156] Still, the countries researched in this report have not just let cyber organically grow in their public sector, but have consciously transferred responsibilities from one department to another in an attempt to improve or rationalize cyber capacity. In 2011, for example, Denmark chose to transfer the role of coordinating cyber security from the ministry of Science, Technology and Innovation to the ministry of Defence. At approximately the same time, Estonia moved in the opposite direction, shifting responsibility for national coordination from Defence to Economic Affairs and Communication. As countries are still in the middle of the process of determining what works and what needs to be further adjusted, it remains difficult to identify good practices. Next to unique political cultures, other aspects such as population size and economy can also impact on national cyber security choices. What might work for Estonia, a Baltic country of 1,4 million people, might not be feasible for the Netherlands with its population of nearly 17 million. Specific institutional arrangements are part of a larger political ecosystem, making the application of potentially successful elements from one ecosystem to a completely different context and environment far from straightforward.

The legal regime is fundamental in determining the place, role and responsibilities of the government institutions involved in national cyber security. Laws grant mandates to government agencies to perform certain missions, and regulate when and under what circumstances infringements on (human) rights can be warranted. This remains a delicate issue as many of the techniques used in cyber defence, such as deep packet inspection, have serious privacy implications. It has not been within the scope of this report to study the different legal regimes in detail, but it has nonetheless become clear that context and timing have played important roles in the development of national laws and regulation. In Estonia and the Czech Republic, cyber crises like the DDoS attacks in 2007 and 2013 provided political momentum and public support for new legal powers in the cyber security field. In Denmark, when the cyber security laws had to be updated, the Snowden revelations broke, significantly complicating the debate. What is undisputed is that the mandates and responsibilities of different public parties in the cyber security field need to be laid down clearly, and that in democratic societies

[156] Boeke, Heinl, and Veenendaal, 'Civil-Military Relations'.

all actions of the government need to permitted by law. This does not apply to private organizations, that need to refrain from breaking laws. Their increased freedom of action and more rapid way of reacting have nonetheless also come under increasing pressure to comply with more complex and extensive data protection laws.

6.1 Fundamental choices

Important in cyber security governance whether there is a bottom-up development of initiatives or more a top-down guidance from the government. Here political culture is of the essence, and although France has not been studied in this research it remains an primary example where the state plays a strong central role in regulating different sectors in society.[157] In Denmark, the role of the CFCS displays a strong top-down element, with the unit responsible for defence against top-level APTs. In this case, Defence or rather the CFCS under its remit, is not a last resort but a first responder. This permits better defence against APTs, a threat that is increasing in scale and sophistication. It does help that the defending intelligence service has multiple sources to harness in its investigations and understands the modi operandi of the perpetrating actors like no other organization. After all, now both the defender and its adversaries are foreign intelligence agencies. In the Netherlands, a culture of consensus and community building has led to a completely different model, whereby the NCSC is at the centre of a hub and spoke model and cooperates with partners on a more equal level, assisting them to help themselves. Estonia and the Czech Republic have a similar construction, but the RIA and NSA do have regulatory tasks and can enforce elements of the notification laws and apply sanctions if necessary. In the Netherlands this responsibility for enforcement lies with the different sectors themselves, permitting the NCSC to concentrate on trust building without being associated with compliance and enforcement measures.

Another choice is between centralizing capacity and establishing a distributed model. In the countries studied in this report, Estonia, and especially the Czech Republic and the Netherlands have a strong distributed model. The Czech Republic has a GovCert, national Cert and CSIRT for military networks, while in Denmark these have all been combined into one. The distributed model fits well with the separate legal regimes and missions of different government functions. However, from a practical perspective, there are some specific drawbacks related to cyber defence. The first concerns databases. Indicators of compromise, malware signatures, or other information on the modus operandi of malicious actors are divided over different centres, leading to duplications and gaps. There is no organization with a complete overview of all the data available, and sharing between organizations remains a continuous process, with stovepipes, cultures and secrecy all exerting a restrictive force on information sharing. The second drawback of a distributed mode concerns personnel. It is already a great challenge for governments to recruit, train and retain qualified IT-personnel, and on financial

[157] Bourcart, '"The State Can't Do Everything Any More"'.

terms they cannot compete with the private sector. Having different centres risks duplicating scarce capacity, and there is a tendency for the most able and talented professionals to gravitate to where the work is most demanding and exciting. This is not monitoring and defence, but intelligence or offence – *if* it has a proper mandate to operate. By clustering capacity, duplication can be avoided and recruitment and training can be organized in a more coherent and efficient way.

	Netherlands	**Denmark**	**Estonia**	**Czech Republic**
Cyber security coordination	Ministry of Security and Justice	Ministry of Defence	Ministry of Economic Affairs & Communication	National Security Authority
Coordination crisis management	Ministry of Security and Justice	Ministry of Defence	Ministry of Interior	Ministry of Interior/ Ministry of Defence
Main public sector CERTs	(NCSC) DefCERT	GovCERT and MilCERT combined in CFSC	CERT-EE	GovCERT, CSIRT.CZ CIRC (defence)
Monitoring government networks	Ministries have own responsibility (NDN)	CFCS conducts Deep Packet Inspection	Ministries have own responsibility	Ministries have own responsibility
Embedding in intelligence community?	Outside NCSC/DCC/DefCERT	Inside	Outside	NSA outside Military inside
Coordination model	PPP Network model, Partnership of equals	PPP, but top-down monitoring	PPP Network model, but enforced compliance	PPP Network model, but enforced compliance
Role Defence in cyber crisis management	Last resort	First responder	Last Resort	Last Resort

The fragmented landscape is most profound within the Netherlands military. DefCERT is tasked with monitoring and defending military networks and systems, and is integrated in for instance the National Response Network, working with the civilian NCSC. From this perspective, DefCERT would be the logical military entity to turn to as a last resort. However, the primary capacity for countering the high-end APTs lies within the Joint Sigint Cyber Unit, and this intelligence unit plays an important role in the National Detection Network. It also has a cyber defence task, and receives information from

international partners on threats to for instance critical infrastructure. Despite possessing the main IOC database and many highly trained malware specialists, its role in cyber crisis management is unclear. At the same time, new cyber capacity is being built up in the Defence Cyber Command, but the mandate for actual deployment of this capacity is not particularly well tailored to the practicalities of cyber offence. The national decision making procedure for the deployment of military assets needs to be followed, which is a lengthy and not very secretive process. While there could be a potential solution in tailoring procedures used for the deployment of Special Forces, there will still be an artificial border between the work and mandate of the intelligence service and that of the DCC. Cyber intelligence is vital for both cyber offence and cyber defence, and the current arrangements are not conductive to effective cooperation.

Governments deliberating in which ministerial department to embed a govCERT, are faced with a binary choice. This is not between a civilian or military option, but whether to organize it inside or outside the intelligence community. Denmark has chosen to embed its GovCERT within the intelligence community, as have for instance the UK and Spain. The Netherlands, Estonia and the Czech Republic have consciously placed their GovCERT (and DefCERT) outside the remit of their intelligence services. This choice has fundamental implications for the partnership relationships that the CERTs will be able to build, and the information they can receive and share. There are therefore two very distinct information-sharing communities, and the natural choice for CERTs is to optimize sharing relationships with partners in their own circle of trust. For example, the primary partner of the Dutch DefCERT is their German military counterpart, which is also institutionally embedded outside the intelligence community. In contrast, the primary partners of the Danish CFCS are to be found inside the international intelligence community. Illustrative is the testimony of a Danish official who worked in the GovCERT when it fell under the remit of the Ministry of Science, Technology and Innovation, and now works for the CFSC within the foreign intelligence service. He acknowledges that he receives much more information now – as a result of embedding in intelligence – than before, and that he can see how partners outside the intelligence community receive relevant reports on cyber security threats much later than those inside, or sometimes not at all. There is of course the counter-argument that private companies are often reluctant to share with the Defence sector, and after Snowden especially with the intelligence sector. In the case of Denmark they have no choice: there is only one centre within the government to cooperate with, and that is the CFCS.

6.2 Common traits

Essential for information sharing relationships, and this is relevant for the preventive as well as reactive phase of crisis management, is the issue of trust. Trust has a face, insofar that it functions between people that know each other, rather than organizational positions that should have a cooperative relationship. Trust also takes a long time to develop, and needs to be sustained by the

parties involved. Besides the central role of trust, the process of information sharing between various involved public and private entities, displays other characteristics of intelligence sharing in general. This concern the quid pro quo concept that implies a give- and-take relationship, and the current (attempted) shift from a 'need to know' to a 'need to share' culture.[158] The former plays to the tendency of intelligence agencies, and by extension their affiliated NCSCs, to only build sharing relationships when there is potential for a return on investment. While logical for international partners, if this is applied to national customers, little will be shared. Using tearlines is an effective way to disseminate information to intelligence consumers in either the public or private sector, but classification levels remain a hurdle for effective information exchange. An often heard criticism of parties that share data with intelligence services is that the information disappears into a black box, with little feedback on what has been done with it. Increasing trust between the intelligence community and the other cyber-security actors should thus be a priority for all partners.

In all reviewed countries, much effort has been invested in identifying and characterizing critical national infrastructure. This has led to improved cyber security awareness, prevention, preparation for crises and resilience. The problem with sectoral delineation, however, is that malicious cyber actors, be it states or criminal groups, will always focus on the weakest link, or approach the target through a trusted connection. The big data breaches at the U.S. company Target and the government's Office of Personnel Management (OPM) both occurred by first breaching the systems of organizations in the supply chain.[159] The accounts and computer systems of high-level targets such as ambassadors or military chiefs have also been compromised through spearfishing campaigns that specifically targeted family members.[160] A sophisticated spear phishing campaign targeting administrative personnel preceded the hack at the Ukraine power station, allowing the intruders to establish a foothold, escalate privileges and install the Black Energy 3 malware.[161] The implications of these examples is that for a determined adversary, anyone linked or even related to a target risks becoming a point of entry. As cyber security is not just a technical affair but also a human awareness one, the attack surface will continue to grow exponentially. As the U.S. Deputy of Chief Cyber within the Department of Justice has aptly described, "you cannot defend yourself out of this problem".[162]

Generic crisis management structures remain leading, with cyber forming a subset in crisis management. In each country the subsidiarity principle applies to crisis management, with the sector (most) struck by the crisis tasked with leading the response. The role of coordinating national crisis management is invested in different departments, just like cyber security, and is also similarly the product of political history and cultures. In Estonia and the Czech Republic the ministries of Interior

[158] Seagle, 'Intelligence Sharing Practices Within NATO'.
[159] Shackleford, 'Combatting Cyber Risks in the Supply Chain'.1
[160] Senior officials at the MIVD and JSCU, interview.
[161] Zetter, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid'.
[162] Newell, 'Most Wanted: Criminalisation of State-Sponsored Activities in Cyberspace'.

are responsible, in Denmark the ministry of Defence, and for the Netherlands the ministry of Security and Justice. In the latter two countries, national crisis management is coordinated by the same ministry that is responsible for coordinating cyber security. This is probably a coincidence, but is potentially helpful when it comes to knowing people and operating in the same ministerial environment and culture. The essence of effective crisis management remains the ability to adopt a flexible organizational response, and integrate expert advice in the decision-making loops. In all countries reviewed, specific advice bodies with cyber expertise have been integrated in the crisis management structures.

Training and exercises are vital for improving preparedness and testing crisis management systems and procedures. At a strategic level, high level policy makers and ministers have been involved in table-top exercises. In Estonia, for example, a recent exercise led to the conclusion that an update of the legal framework was necessary. Large-scale EU and NATO exercises, such as Cyber Europe or CMX, not only test national institutions well, but have also given the multinational departments that organize and run these exercises unique insights into which national systems and institutions work well in which situations, and what good practices can be distilled in cyber crisis management. On a tactical and operational level, exercises such as Locked Shields test and improve the skills of the defenders, and potentially lift the baseline of the quality of all participating teams. Ideally the teams that participate in the exercise also function as a team in their daily work, but in practice some countries compose their teams from different national institutions. The concept of Rapid Reaction Teams, as has been institutionalized by Denmark (and NATO), can offer a tailored and effective response. If the public sector itself does not itself possess the scarce IT-talent required, it can still assist by facilitating the deployment of experts to the crisis location. An example would be to use military helicopters to deploy private-sector IT-specialists to where they are urgently needed.

6.3 Conclusion

This research has had certain limitations. From a methodological perspective, there has been an imbalance in the information available for the different case studies, although it has been a conscious choice to work out the Netherlands in more detail as a reference model for the others. There is a large divide between academia and policy on elements of cyber defence, and despite frank and helpful interviews with officials of each country studies, many details of cyber crisis management remain classified, politically sensitive or both. From a substantive point of view, the cyber security and crisis management institutions and arrangements are part of a complex ecosystem, with many interdependent variables. In Denmark, for example, top-down monitoring protects government networks from APTs, while in the Netherlands different cyber challenges are met by different public-private partnerships, on the base of equality. The lack of top-down control is balanced by strong bottom-up initiatives, such as the well-developed ISACs. This is not the case in Denmark, where there

is less need or desire to develop ISACs. Finally, the choice of country studies in this report provides a good coverage of small to medium European countries, but raises important new questions. For instance, how have the United Kingdom, France and Germany, as Europe's main security powers, organized their cyber crisis management structures?

The countries researched in this report have made a clear choice on whether to consider Defence as a first responder or a last resort in cyber crisis management. The ministry of Defence only has a prominent in Denmark, where the CFCS provides first response capacity in incident and crisis management. For the Netherlands, the Czech Republic and Estonia, Defence is seen as a last resort, but in each country it is still unclear precisely when and under what circumstances military cyber capacity can be called upon. Of course, crisis situations can never completely be foreseen and a flexible response by all departments is warranted. But for a military which is used to preparing for every possible eventuality, a clearer indication of its potential role is desirable. In Estonia the Cyber Defence Unit of the Estonian Defence League is an interesting concept in development, but probably difficult to scale. Much rests on the volunteer element and the informal networks of trusted professionals. In the Netherlands, the multi-stakeholder partnership model has succeeded in significantly raising the baseline of cyber security (awareness and preparation) and facilitating cooperation and assistance in times of crisis. Although in the ministry of Defence DefCERT would be the first in line to provide assistance to civilian authorities, its other organisations with significant cyber defence capacity could equally contribute and would benefit from a more clearly defined role in times of crisis.

7 Acknowledgements

First and foremost I would like to thank Thomas Brzezinski, who provided invaluable assistance in researching and drafting this paper. His sharp reasoning and eye for detail has been much appreciated.

I am grateful to the officials at the Danish Centre for Cyber Security for receiving me so well in Copenhagen. I would also like to thank the officials in the Czech NSA and Estonia's RIA for their time and patience in answering my questions. Kadri Kaska, from NATO's CCD COE, has provided much help in the Estonian case-study. On the Dutch side, we are grateful to Eric Luijf, the head of DefCERT, policy officers at the National Cyber Security Centre and officials in the intelligence community and Defence Cyber Command, for their time and insights.

This research was made possible by the Netherlands ministry of Defence and the ministry of Security and Justice.

8 References

‘2015 Annual Report of the Estonian Information System Authority’s Cyber Security Branch’, n.d. https://www.ria.ee/public/Kuberturvalisus/RIA-Kyberturbe-aruanne-2014_ENG.pdf.

Addae, Richard, Jetske Hebbink, and Sven Hamelink. ‘De herijking vitale infrastructuur Nederland: Een veranderende wereld vraagt om een mee veranderend beleid’. *Magazine Nationale Veiligheid en Crisisbeheersing*, 2015.

Algemene Inlichtingen- en Veiligheidsdienst. *Jaarverslag 2015*. Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties - Algemene Inlichtingen- en Veiligheidsdienst, 2016. https://www.aivd.nl/publicaties/jaarverslagen/2016/04/21/jaarverslag-aivd-2015.

Andrš, Jan. ‘Czech Cyber Security: Finally ahead of Europe?’ Blog post. *SVAT Cyber Security*, 4 November 2014. http://www.nfgsvat.com/czech-cyber-security-finally-ahead-of-europe/#.V0P_gORN-X8.

‘Annual Review 2015 Estonian Internal Security Service’, 2015. https://www.kapo.ee/en/content/annual-reviews.html.

Arnold, Kraesten, and Paul Ducheine. ‘Besluitvorming bij cyberoperaties’. *Militare Spectator*, 20 February 2015. http://www.militairespectator.nl/thema/recht-cyberoperations/artikel/besluitvorming-bij-cyberoperaties.

Bauer, Johannes M., and Michel J.G. van Eeten. ‘Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options’. *Telecommunications Policy* 33, no. 10–11 (November 2009): 706–19. doi:10.1016/j.telpol.2009.09.001.

Boeke, Sergei, Caitriona H. Heinl, and Matthijs A. Veenendaal. ‘Civil-Military Relations and International Military Cooperation in Cyber Security: Common Challenges & State Practices across Asia and Europe’, 69–80. Tallinn: IEEE, 2015. doi:10.1109/CYCON.2015.7158469.

Boin, Arjen, ed. *Crisis Management*. Vol. 2. 3 vols. Los Angeles, CA: SAGE, 2008.

Boin, Arjen, and Fredrik Bynander. ‘Explaining Success and Failure in Crisis Coordination’. *Geografiska Annaler: Series A, Physical Geography* 97, no. 1 (March 2015): 123–35. doi:10.1111/geoa.12072.

Boin, Arjen, and Allan McConnell. ‘Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience’. *Journal of Contingencies and Crisis Management* 15, no. 1 (2007): 50–59.

Boin, Arjen, and Paul ’t Hart. ‘Organising for Effective Emergency Management: Lessons from Research’. *Australian Journal of Public Administration* 69, no. 4 (December 2010): 357–71. doi:10.1111/j.1467-8500.2010.00694.x.

Boivin, Alexandra. *The Legal Regime Applicable to Targeting Military Objectives in the Context of Contemporary Warfare*. Research Paper Series, No. 2/2006. Geneva: Geneva Academy of International Humanitarian Law and Human Rights, 2006. http://www.geneva-academy.ch/docs/publications/collection-research-projects/CTR_objectif_militaire.pdf.

Bourcart, Léo. ‘“The State Can’t Do Everything Any More”: Understanding the Evolution of Civil Defence Policies in France’. *Resilience* 3, no. 1 (2 January 2015): 40–54. doi:10.1080/21693293.2014.988913.

Britz, Malena. ‘Translating EU Civil Protection in the Nordic States – towards a Theoretical Understanding of the Creation of European Crisis Management Capacities.’, 2007. http://aei.pitt.edu/7714/1/britz-m-11d.pdf.

Broeders, Dennis. *Investigating the Place and Role of the Armed Forces in Dutch Cyber Security Governance*. Department of Sociology, Erasmus University of Rotterdam, 2014. https://www.researchgate.net/profile/Dennis_Broeders/publication/280522039_Investigating_the_Place_and_Role_of_the_Armed_Forces_in_Dutch_Cyber_Security_Governance/links/55b74c8008aed621de045985.pdf.

Cardash, Sharon L., Frank J. Cilluffo, and Rain Ottis. ‘Estonia’s Cyber Defence League: A Model for the United States?’ *Studies in Conflict & Terrorism* 36, no. 9 (1 September 2013): 777–87. doi:10.1080/1057610X.2013.813273.

Carey III, Casimir. ‘The International Community Must Hold Russia Accountable for Its Cyber Militias’. *Small Wars Journal*, 27 March 2013. http://smallwarsjournal.com/jrnl/art/the-international-community-must-hold-russia-accountable-for-its-cyber-militias.

Carr, Madeline. ‘Public-Private Partnerships in National Cyber-Security Strategies’. *International Affairs* 92, no. 1 (2016): 43–62. doi:10.1111/1468-2346.12504.

Centre for Cyber Security. ‘The Danish Cyber and Information Security Strategy’. Danish Defence Intelligence Service, February 2015. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/danish-cyber-and-information-security-strategy/view.

———. ‘Threat Assessment - The Cyber Threat against Denmark’. Centre for Cyber Security, January 2016. https://fe-ddis.dk/cfcs/CFCSDocuments/Threat%20Assessment%20-%20The%20cyber%20threat%20against%20Denmark.pdf.

Clark, Kas, Don Stikvoort, Eelco Stofbergen, and Elly van den Heuvel. ‘A Dutch Approach to Cybersecurity through Participation’. *IEEE Security & Privacy* 12, no. 5 (October 2014): 27–34. doi:10.1109/MSP.2014.83.

Corera, Gordon. *Intercept: The Secret History of Computers and Spies*. W&N, 2015.

Cyber Security Raad. *CSR - Cyber Security Raad*. Brochure. Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid. Accessed 22 April 2016. http://cybersecurityraad.nl/assets/flyer-csr_v7_web.pdf.

‘Cyber Security Strategy 2014-2017’. Ministry of Economic Affairs and Communication, 2014. https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.

‘Danish Comments on GREEN PAPER on a European Programme for Critical Infrastructure Protection (Presented by the Commission)’, 2 December 2005. http://www.ft.dk/samling/20051/almdel/reu/spm/193/svar/230261/250944.pdf.

Danish Defence Commission. *Danish Defence - Global Engagement*. Copenhagen: Danish Ministry of Defence, 2009. http://www.fmn.dk/videnom/Documents/Summary-Report_Danish_Defence_Commission_June2009.pdf.

Danish Emergency Management Agency. *Crisis Management in Denmark*. Birkerød: Danish Emergency Management Agency, 2015. http://brs.dk/viden/publikationer/Documents/Crisis%20Management%20in%20Denmark_UK.pdf.

Dinstein, Yoram. ‘Legitimate Military Objectives under the Current Jus in Bello’. In *Legal and Ethical Lessons of NATO’s Kosovo Campaign*, edited by Andru E. Wall, 78:139–72. International Law Studies. Newport, RI: U.S. Naval War College, 2003. https://www.usnwc.edu/Research---Gaming/International-Law/New-International-Law-Studies-%28Blue-Book%29-Series/International-Law-Blue-Book-Articles.aspx?Volume=78.

Dunn-Cavelty, Myriam, and Manuel Suter. ‘Public–private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection’. *International Journal of Critical Infrastructure Protection* 2, no. 4 (December 2009): 179–87. doi:10.1016/j.ijcip.2009.08.006.

Dynes, Russel R., and B.E. Aguirre. ‘Organizational Adaptation to Crises: Mechanisms of Coordination and Structural Change’. In *Crisis Management*, edited by Arjen Boin, II:320–25. Los Angeles, CA: SAGE, 2008.

Fox-IT. *Black Tulip: Report of the Investigation into the DigiNotar Certificate Authority Breach*. Delft: Fox-IT, 2012. https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf.

Harris, Shane. *@WAR : The Rise of the Military-Internet Complex*. Boston: Houghton Mifflin Harcourt, 2014.

Head of DefCERT. interview, 19 February 2016.

Healey, Jason, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Vienna, VA: Cyber Conflict Studies Association, 2013. https://books.google.nl/books/about/A_Fierce_Domain.html?id=zaYHnQEACAAJ&redir_esc=y.

Hellenberg, Timo, and Pekka Visuri. ‘Analysis of Civil Security Systems in Europe Country Study Estonia’. Anvil Project, June 2013. http://anvil-project.net/wp-content/uploads/2013/12/Estonia_v1.0.pdf.

Inspectie Veiligheid en Justitie. *Rapport: Evaluatie van de rijkscrisisorganisatie tijdens de DigiNotar-crisis*. Den Haag, 2012. https://www.rijksoverheid.nl/documenten/rapporten/2012/06/28/evaluatie-van-de-rijkscrisisorganisatie-tijdens-de-diginotar-crisis.

Jackson, Camille Marie. ‘Estonian Cyber Policy After the 2007 Attacks: Drivers of Change and Factors for Success’. *New Voices In Public Policy* 7, no. 1 (19 April 2013). doi:10.13021/nvpp.v7i1.69.

Järvinen, Heini. ‘Danish Government Plans to Create a Center for Cybersecurity with Privacy-Invasive Powers’. *EDRi*, 12 March 2014. https://edri.org/danish-government-plans-create-center-cybersecurity-privacy-invasive-powers/.

Jochem, Aart, and Anouk Vos. ‘Het Nationaal Response Netwerk: Een virtuele bucket line’. *InformatieBeveiliging Magazine*, 2014.

Kadlecova, Lucie. ‘Presentation Cyber in the National Crisis Management System: The Czech Republic’. presented at the CyCon, Tallinn, Estonia, 31 May 2016.

Kaska, Kadri. *National Cyber Security Organisation: The Netherlands*. Tallinn: NATO CCD COE, 2015. https://ccdcoe.org/multimedia/national-cyber-security-organisation-netherlands.html.

Kaska, Kadri, Anna-Maria Osula, and Jan Stinissen. *The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis*. Tallinn, Estonia: NATO CCD COE, 2013. https://www.ccdcoe.org/multimedia/cyber-defence-unit-estonian-defence-league-legal-policy-and-organisational-analysis-0.

Knights, Michael. ‘Operation Iraqi Freedom’. In *Operation Iraqi Freedom and the New Iraq: Insights and Forecasts*, edited by Michael Knights, 27–74. Washington, DC: Washington Institute for Near East Policy, 2004. https://www.washingtoninstitute.org/uploads/Documents/pubs/OperationIraqiFreedom.pdf.pdf.

Kosek, Miroslav. ‘Crisis Management in the Czech Republic’. presented at the DCAF Whole-of-Government Course on Security Sector Governance and Oversight, Ohrid, Macedonia, 7 April 2009. http://www.dcaf.ch/content/download/34699/524615/version/1/file/Crisis%2520Management%2520in%2520the%2520Czech%2520Republic%2520by%2520M%2520Kosek.pdf.

Kostyuk, Nadiya. ‘International and Domestic Challenges to Comprehensive National Cybersecurity: A Case Study of the Czech Republic’. *Journal of Strategic Security* 7, no. 1 (March 2014): 68–82. doi:10.5038/1944-0472.7.1.6.

Kouremetis, Michael. ‘An Analysis of Estonia’s Cyber Security Strategy, Policy and Capabilities’. In *Proceedings of the 14th European Conference on Cyber Warfare and Security 2015*, 404–12. Reading, UK: Academic Conferences and Publishing International, 2015. https://books.google.nl/books/about/ECCWS2015_Proceedings_of_the_14th_Europe.html?hl=nl&id=BzQ7CgAAQBAJ&q=kouremetis.

Kovoor-Misra, Sarah, and Manavendra Misra. ‘Understanding and Managing Crises in an “Online World”’. In *International Handbook of Organizational Crisis Management*, edited by Christine M. Pearson, Christophe Roux-Dufort, and Judith A. Clair, 85–104. London: Sage, 2007. http://dx.doi.org/10.4135/9781412982757.n3.

Libicki, Martin C., Lillian Ablon, and Tim Webb. *The Defender’s Dilemma Charting a Course Toward Cybersecurity*. Santa Monica, CA: RAND Corporation, 2015. http://www.rand.org/pubs/research_reports/RR1024.html.

Luiijf, Eric. principal consultant at TNO, interview, 11 March 2016.

———. ‘The Netherlands’. In *Cyber Conflicts and Small States*, edited by Lech J. Janczewski and William Caelli, chapter 7. Farnham, Surrey: Routledge, 2015.

Luiijf, Eric, and Jason Healey. ‘Organisational Structures & Considerations’. In *National Cyber Security Framework Manual*, edited by Alexander Klimburg, 108–45. Tallinn: NATO CCD COE, 2012.

Mad’ar, Tomáš. *Aiming for the Stars: An Ambitious Czech Cybersecurity Approach*. Briefing Paper, 2/2015. Association for International Affairs, 2015. http://www.amo.cz/wp-content/uploads/2015/11/amocz_bp-2015_02.pdf.

Mansfield-Devine, Steve. ‘Estonia: What Doesn’t Kill You Makes You Stronger’. *Network Security* 2012, no. 7 (July 2012): 12–20. doi:10.1016/S1353-4858(12)70065-X.

Marshall Jr., Tyrone. ‘New DoD Cyber Strategy Nears Release, Official Says’. *U.S. DEPARTMENT OF DEFENSE*, 14 April 2015. http://www.defense.gov/News-Article-View/Article/604456/new-dod-cyber-strategy-nears-release-official-says.

Matlary, Janne Haaland, and Øyvind Østerud. *Denationalisation of Defence: Convergence and Diversity*. Ashgate, 2013.

Minárik, Tomáš. *National Cyber Security Organisation: Czech Republic*. 2nd ed. Talinn: NATO CCD COE, 2016. https://www.ccdcoe.org/multimedia/national-cyber-security-organisation-czech-republic.

Ministerie van Defensie. ‘Actualisering Defensie Cyber Strategie’. Brief van de minister van Defensie, TK 2014-15, 33321-5, 23 February 2015. https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2015Z03083&did=2015D06376.

———. Brief van de minister van Defensie. ‘Voortgangsrapportage over de uitvoering van de Defensie Cyber Strategie’. Brief van de minister van Defensie, TK 2015-16, 33321-7, Brief van de minister van Defensie, 15 March 2016.

Ministerie van Veiligheid en Justitie. *National Cyber Security Strategy 2: From Awareness to Capability*. The Hague: National Coordinator for Security and Counterterrorism, 2013. https://www.ncsc.nl/english/current-topics/national-cyber-security-strategy.html.

———. *National Cyber Security Strategy (NCSS): Strength through Cooperation*. The Hague, 2011. https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/news/national-cyber-security-strategy-launched/1/The%2BNational%2BCyber%2BSecuriry%2BStrategy%2B%2BNCSS%2B%2B2011.pdf.

———. *Nationale Cybersecurity Strategie 2: Van bewust naar bekwaam*. The Hague: Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2013. https://www.rijksoverheid.nl/documenten/rapporten/2013/10/28/nationale-cyber-security-strategie-2.

———. ‘Presentatie Nationaal Detectie Netwerk’. 12 September 2013. https://www.rijksoverheid.nl/documenten/wob-verzoeken/2013/09/12/presentatie-nationaal-detectie-netwerk.

Ministry of Defence of the Czech Republic. *The Long Term Perspective for Defence 2030*. Prague: Ministry of Defence of the Czech Republic - Military History Institute (MHI). Accessed 3 June 2016. http://www.army.cz/images/id_8001_9000/8503/THE_LONG_TERM_PERSPECTIVE_FOR_DEFENCE_2030.pdf.

Nationaal Coördinator Terrorismebestrijding en Veiligheid. *Nationaal Crisisplan ICT*. Den Haag: Ministerie van Veiligheid en Justitie, 2012. https://www.rijksoverheid.nl/documenten/rapporten/2012/11/13/nationaal-crisisplan-ict.

———. *Nationaal handboek crisisbesluitvorming*. Den Haag: Ministerie van Veiligheid en Justitie, 2013. https://www.rijksoverheid.nl/documenten/kamerstukken/2013/04/27/nationaal-handboek-crisisbesluitvorming.

———. ‘Resultaten herijking vitale infrastructuur’. Factsheet. The Hague: Ministerie van Veiligheid en Justitie, July 2015.

National Cyber Security Centre. *Action Plan for the National Cyber Security Strategy of the Czech Republic for the Period from 2015-2020*. National Security Authority. Accessed 4 May 2016. https://www.govcert.cz/download/nodeid-590/.

———. *National Cyber Security Strategy of the Czech Republic for the Period from 2015-2020*. National Security Authority, 2015. https://www.govcert.cz/en/info/strategy-a-action-plan/.

‘National Security Concept of Estonia’, 12 May 2010. http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_of_estonia.pdf.

Newell, Sean. ‘Most Wanted: Criminalisation of State-Sponsored Activities in Cyberspace’. presented at the CyCon, Tallinn, Estonia, 1 June 2016.

O’Dwyer, Gerard. ‘Denmark To Develop Offensive Cyber Capability’. *Defense News*, 8 January 2015. http://www.defensenews.com/story/defense/policy-budget/cyber/2015/01/08/denmark-cyber-hackers-china-terma/21448705/.

Official at CCDCOE. personal communications, n.d.

Officials at the National Security Authority. interview, 2 April 2016.

———. personal communications, n.d.

Officials within the Danish Centre for Cybersecurity (CFCS). interviews Copenhagen, 3 May 2016.

Onderzoeksraad voor Veiligheid. *Het DigiNotarincident: Waarom digitale veiligheid de bestuurstafel te weinig bereikt*. Den Haag: De Onderzoeksraad voor Veiligheid, 2012. http://www.onderzoeksraad.nl/nl/onderzoek/1094/het-diginotarincident.

Osula, Anna-Maria. *National Cyber Security Organisation: Estonia*. Tallinn, Estonia: NATO CCD COE, 2015. https://www.ccdcoe.org/multimedia/national-cyber-security-organisation-estonia.

Padar, Andrus. 'The Estonian Cyber Defence Unit'. presented at the Roundtable Civil Military Relations in Cyberspace, Singapore, 18 November 2014.

Pearson, Christine M., and Judith A. Clair. 'Reframing Crisis Management'. In *Crisis Management*, edited by Arjen Boin, II:1–24. Los Angeles, CA: SAGE, 2008.

Roux-Dufort, Christophe. 'A Passion for Imperfections: Revisiting Crisis Management'. In *International Handbook of Organizational Crisis Management*, edited by Christine M. Pearson, Christophe Roux-Dufort, and Judith A. Clair, 221–52. Thousand Oaks: SAGE, 2007. http://dx.doi.org/10.4135/9781412982757.n8.

———. 'A Passion for Imperfections: Revisiting Crisis Management'. In *International Handbook of Organizational Crisis Management*, edited by Christine M. Pearson, Christophe Roux-Dufort, and Judith A. Clair, 221–52. Thousand Oaks: SAGE, 2007. http://dx.doi.org/10.4135/9781412982757.n8.

Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013. http://ebooks.cambridge.org/ref/id/CBO9781139169288.

Seagle, Adriana N. 'Intelligence Sharing Practices Within NATO: An English School Perspective'. *International Journal of Intelligence and CounterIntelligence* 28, no. 3 (3 July 2015): 557–77. doi:10.1080/08850607.2015.1022468.

Senior official at Defence Cyber Command. interview, n.d.

Senior officials at the MIVD and JSCU. interview, n.d.

Senior officials at the National Cyber Security Centre. Interview, n.d.

Shackleford, Dave. 'Combatting Cyber Risks in the Supply Chain'. A SANS Whitepaper. SANS, September 2015.

'State-Sponsored Hackers Spied on Denmark'. *The Local DK*, 22 September 2014. http://www.thelocal.dk/20140922/denmark-was-hacked-by-state-sponsored-spies.

Stone, Brad, and Michael Riley. 'Mandiant, the Go-To Security Firm for Cyber-Espionage Attacks'. *Bloomberg.com*, 8 February 2013. http://www.bloomberg.com/news/articles/2013-02-07/mandiant-the-go-to-security-firm-for-cyber-espionage-attacks.

't Hart, Paul, Uriel Rosenthal, and Alexander Kouzmin. 'Crisis Decision Making: The Centralization Thesis Revisited'. *Administration & Society* 25, no. 1 (May 1993): 12–45. doi:10.1177/009539979302500102.

Taskforce Bestuur & Informatieveiligheid Dienstverlening. 'Voortgangsrapportage', February 2013. https://www.rijksoverheid.nl/documenten/rapporten/2014/12/01/voortgangsrapportage-taskforce-bestuur-informatieveiligheid-dienstverlening.

Torenvlied, R., E. Giebels, R.A. Wessel, J.M. Gutteling, M. Moorkamp, and W.G. Broekema. *Evaluatie nationale crisisbeheersingsorganisatie vlucht MH17*. WODC. Enschede: Universiteit Twente, 2015. https://www.wodc.nl/onderzoeksdatabase/2563-evaluatie-crisisbeheersingsorganisatie-vlucht-mh17.aspx?nav=ra&l=veiligheid_en_preventie&l=veiligheid.

UN General Assembly. ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’. Resolution A/68/98, 24 June 2013. http://undocs.org/A/68/98.

Vykopal, Jan, and Ondřej Mokoš. ‘Czech Cyber Defence Exercise: Lessons Learned’. presented at the FIRST/TF-CSIRT Technical Colloquium, Prague, 26 January 2016. https://www.terena.org/activities/tf-csirt/meeting47/J.Vykopal-O.Mokos-Czech-lessons.pdf.

Wall, Andru E., ed. *Legal and Ethical Lessons of NATO’s Kosovo Campaign*. Vol. 78. International Law Studies. Newport, RI: U.S. Naval War College, 2003. https://www.usnwc.edu/Research---Gaming/International-Law/New-International-Law-Studies-%28Blue-Book%29-Series/International-Law-Blue-Book-Articles.aspx?Volume=78.

Wyman, Joanna Stone. ‘Emergency Management in Denmark: Lessons Learned At Home and Abroad’. In *Comparative Emergency Management Book*. FEMA - Emergency Management Institute, n.d. https://www.training.fema.gov/hiedu/aemrc/booksdownload/compemmgmtbookproject/.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon*. New York: Crown, 2014.

———. ‘Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid’. *WIRED*, 3 March 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.