The governance of cybersecurity

Adams, Samantha; Brokx, Marlou; Dalla Corte, Lorenzo; Savic, Masa; Kala, Kaspar; Koops, Bert-Jaap; Leenes, Ronald; Schellekens, Maurice; E Silva, Karine; Skorvánek, Ivan

The Governance of Cybersecurity

A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK

Samantha A. Adams
Marlou Brokx
Lorenzo Dalla Corte
Maša Galič
Kaspar Kala
Bert-Jaap Koops
Ronald Leenes
Maurice Schellekens
Karine e Silva
Ivan Škorvánek

Tilburg University
TILT – Tilburg Institute for Law, Technology, and Society
P.O. Box 90153
5000 LE Tilburg
The Netherlands
<s.a.adams@uvt.nl>

November 2015

Colophon

Authors
Samantha A. Adams
Marlou Brokx
Lorenzo Dalla Corte
Maša Galič
Kaspar Kala
Bert-Jaap Koops
Ronald Leenes
Maurice Schellekens
Karine e Silva
Ivan Škorvánek

Publisher
Tilburg University
TILT – Tilburg Institute for Law, Technology, and Society
P.O. Box 90153
5000 LE Tilburg
The Netherlands

Commissioned by
WODC, Ministry of Security & Justice
Turfmarkt 147
2511 DP The Hague
The Netherlands

Date
November 2015

Table of Contents

Summary

Society's increased dependency on networked technologies and infrastructures in nearly all sectors poses a new challenge to governments and other actors to ensure the sustainability and security of all things 'cyber'. Cybersecurity is a particularly complex field, where multiple public and private actors must work together, often across state borders, not only to address current weaknesses, but also to anticipate and prevent or pre-empt a number of different kinds of threats. This report examines how public policy and regulatory measures are used to organise such processes in five countries: Canada, Estonia, Germany, the Netherlands and the UK.

The contextual framework guiding this analysis first attempts to define cybersecurity, combining a grammatical understanding of the component parts 'cyber' and 'security', a hermeneutic understanding of related terms and a pragmatic understanding of how 'cybersecurity' is used in practice. Cybersecurity is defined as the proactive and reactive processes working toward the ideal of being free from threats to the confidentiality, integrity, or availability of the computers, networks, and information that form part of, and together constitute, cyberspace—the conceptual space that affords digitised and networked human and organisational activities. With this working definition of cybersecurity in place, the framework also identifies developments in the theoretical understanding of 'governance', first by looking at the shift from government to governance, then at the relationship between governance and regulation, and finally at more recent theories that recognize multiple forms and centres of governance, as well as the iterative and sometimes experimental nature of governance processes. Recent work on risk governance is also especially relevant to this particular case. Thus, 'cybersecurity governance' broadly refers to the approaches used by multiple stakeholders to identify, frame and coordinate cybersecurity.

This study constitutes a 'quick scan' of relevant policy and initiatives using a comparative case-oriented policy and stakeholder analysis. The five countries were selected on the basis of geographic diversity, different legal traditions, presence of a national cybersecurity strategy, a high ranking on the ICT Development Index and availability of sources. For each country an analysis was made of cybersecurity governance in three areas: botnet mitigation, protection of vital infrastructures and protection of identity infrastructures. The cases were selected to be diverse, and to cover the main aspects of cybersecurity (confidentiality, availability and integrity), different domains of government (law enforcement, national security, and service delivery), and different levels of private-actor involvement.

The botnet case examines mitigation efforts with regard to machines infected by bots (pieces of advanced malicious software that install system backdoors that connect back to remote machines via common communication channels). Botnets have become complex, resilient infections, remaining under the radar of security tools such as firewalls and anti-viruses. All of the countries

included in this quick scan have a national Computer Emergency Response Team (CERT), which has a clear oversight mandate regarding the dissemination of threats on national territory. While the procedures followed by CERTs are to a large extent harmonised, the practical value of their operations in regard to botnets varies largely. Many CERTs distribute relevant information within circles of trust, but such information often remains undisclosed to a larger audience. Multi-stakeholder mitigation efforts also seem to vary, while all countries have demonstrated participation in international cooperative efforts against botnets. There is a significant level of international cooperation in botnet mitigation, which is facilitated by the fact that all countries in our study have ratified the Cybercrime Convention. Legislation is thus a harmonizing element in this case. However, because the Convention acts as a minimum catalogue of offences and investigation powers, significant differences between countries' law remain. An important point to be addressed is the fact that ISPs are currently quite limited in the types of action they can take. There are attempts to formalize an increased role for ISPs, but this is largely through ISPs taking the initiative to change their Terms of Use.

Vital infrastructures are examined through the lens of the energy sector, as this sector has had a number of high-profile incidents related to (among others) technical malfunctioning and human error that demonstrate the importance of good cybersecurity governance. Although this narrows the focus with regard to vulnerabilities in and governance of vital infrastructures, the quick scan revealed that part of the problem across the board lies in the broad definition of what constitutes a country's 'vital' infrastructures. The combination of numerous policy documents containing generally vague recommendations, with a large, and growing, number of actors that are somehow related to the governance of vital infrastructures, make the field hard to oversee for governance purposes. Further, this case highlights that economic factors play an important role, as the distribution of responsibilities among public and private parties, and the consequent strength or weakness of obligations of parties, partly depends on how resources are allocated and on parties' willingness to invest in preventive measures that serve a combination of public and private interests. Even more importantly, the case illustrates the need for coordination in the governance of cybersecurity: the choice of new measures to take touches upon the general interest and therefore legitimises certain government involvement in stipulating the responsibilities of private actors. In the cases discussed here, two types of institutionalization can be discerned: institutionalization in the energy domain and institutionalization in the cybersecurity domain. It also shows how the theoretical notion of governance-as-process takes shape in practice in the institutionalization of both the energy domain and the cybersecurity domain. The role of the state with regard to governance of this sector often takes on the form of providing a framework of rules within the boundaries of which private actors are allowed to act, which helps raise major players' awareness of potential security risks, but should at the same time be approached carefully, as this can potentially create too much red tape.

The identity infrastructures reviewed in this quick scan are quite new, with most still being developed. As with the previous cases, the distributed responsibility and mutual dependency between actors is evident as they attempt to ensure the protection of individual privacy and citizen-specific data. There are four primary issues relevant to governance of these infrastructures: 1) architecture and interoperability (with different approaches, from centralised infrastructures to decentralised approaches requiring interoperability), 2) the role of citizen engagement in identification systems (transparent communication strategies when implementing identification infrastructures, and empowering users to protect their identity, being important factors), 3) combating fraud and other potential threats (with countries experiencing different types and levels of abuse) and 4) the role of regulatory measures (with legislation playing a relatively less prominent role, while the high degree of mutual dependence between the different actors provides strong legitimisation for regulatory intervention). How the different countries deal with these issues exemplifies both the trial-and-error nature of experimentalist governance and many of the tensions associated with risk governance. Rather than restricting the capacity of traditional authority as is stated in these governance theories, however, how these infrastructures are developing highlights areas where traditional governance strategies such as regulation fall short, e.g., in creating a security-oriented mentality, but at the same time also legitimize the need for more clarity of roles, which can be offered through regulatory (legislative) measures that clarify roles rather than leaving decisions to the discretion of multiple actors.

Reviewing these findings, we can draw some conclusions on the distribution of responsibilities and the role of law and other forms of regulation in cybersecurity governance. The distribution of responsibilities shows many examples of polycentric governance, with varying constellations of actors being involved in different sub-fields of cybersecurity. National government agencies responsible for the primary agenda-setting and coordination efforts range from ministries of security and justice, defence, and economic affairs. It is less clear to what degree each of the agencies in the lead has an identified coordinator status with a given final decision-making authority; the coordination role seems better described as one of providing guidance, promoting best practices and engaging in activities to facilitate collaboration with and between other actors. Whereas the distribution of authority across sectors and many levels of government could potentially be problematic from a governance perspective, cybersecurity, particularly in case of critical infrastructure protection at the national level, is a key issue that is increasingly seen as a joint task of society at large, suggesting more distribution of responsibilities across sectors, levels of government and types of individual and corporate actors. The involvement of private actors in voluntary cooperation schemes requires attention, because of the influence of economic factors; it is important that policy choices for new measures in polycentric arrangements (and thus who is responsible for new measures and who should invest in them) factor in the general interest, which may legitimise, depending on the context, stronger government involvement. A polycentrically governed cybersecurity landscape raises more challenges than only dealing with the mutual interdependence between public and private actors, however. The cases show that counteracting the security threats posed to the various infrastructures is rarely a merely technical solution; rather, communication is a key part of governance processes, be it informing the affected parties after the fact or raising public awareness as part of preventive strategies. Moreover, they all point to the need for reflexivity and iterative learning in governance processes, which is especially critical given the dynamic nature of the cybersecurity landscape and the fact that actors cannot always foresee and oversee all the possible threats and their consequences.

When it comes to the role of law and other forms of regulation, we can conclude that the regulatory framework of cybersecurity has certain international elements, e.g., in cybercrime legislation and technical standards, but is largely undertaken at the national (and sometimes sub-national) level. Supranational regulation is visible in the EU, but rather limited to certain aspects of cybersecurity, such as critical infrastructures and telecommunications regulation. Although policy learning or legal transplants might take place, which we cannot determine on the basis of a quick scan, it is clear that a comprehensive global regulatory effort to cybersecurity is not visible in the cases we studied. A similar observation can be made at the national level: most cybersecurity regulation is relatively specific, covering a particular aspect of cyberspace or of security, or cybersecurity in a particular context. Comprehensive regulatory frameworks are rare – understandably so, given the complexity of cybersecurity. Moreover, law is not the only regulatory instrument in cybersecurity, although it plays an important role in all areas, as a general framework or as backstop regulation for situations that cannot be dealt with by private regulation alone. Legal frameworks are supplemented by, or – more often – expanded and detailed in, lower forms of regulation, such as administrative codes or (technical) standards, which may be explicitly made mandatory through a law as a minimum level of security or implicitly incorporated through a reference to open norms. Thus, cybersecurity regulation is often layered regulation, with more general legislative legal norms and more concrete lower-level norms. In several cases, soft law can also be observed that is not necessarily part of an overarching legislative framework, in the form of agreements between stakeholders, sectoral guidelines or principles that serve as reference points for organisations or professionals, or contracts between public and private parties, where Terms & Conditions play an additional role in the governance of behaviour. Particularly in the identification infrastructures case, we can see the role of the state shift from being (only or largely) a public-policy maker and coordinator of society to being (also) one stakeholder among many with an interest in governance.

To put our findings into perspective, and to assist policy-makers in addressing the challenges raised by a complex, not fully overseeable and not fully overseen, landscape of polycentric cybersecurity governance, we refer to two concepts from critical literature on cybersecurity governance that can help avoid tendencies toward overblown or inefficient measures (‘hypersecuritisation’), and thus might help achieve a balanced and realistic approach to cybersecurity governance. First, the approach of the ‘cybersecurity ladder’, which considers the likelihood of a cyberattack and the damage it might involve, argues that thinking about and planning for worst-case scenarios (the top of the ladder in the air), such as cyberwarfare or cyberterrorism, is a legitimate task of national security, but that this should not receive too much attention at the expense of more plausible cyberproblems (the bottom of the ladder that is firmly grounded). The focus should be on types of attacks that are more likely and even common, such as cybercrime, cyberespionage and attacks on critical infrastructures. Second, the 'balanced risk approach' deals with cybersecurity through the lens of risk governance, involving realistic risk assessment, risk management and risk communication. While there is a need for proactive solutions that ensure stability over the longer term, at the same time it is important to avoid over-comprehensive approaches (i.e. securing everything Internet) that lack focus and concrete goals. This involves avoiding rhetorical or emotional responses that are frequently visible in cybersecurity discourse, referring to hypothetical disasters that are not evidence-based, but instead conducting a rational risk analysis of the threats presented by cybersecurity in terms of (1) calculating the cost per saved life; (2) defining a level of acceptable risk; (3) applying a cost-benefit analysis; and (4) adequate communication about taken measures and residual, accepted risks.

Based on use cases and literature, we identified the following six 'lessons learned', or points for further consideration.

1. Do not expect to resolve issues merely by establishing more laws. States currently tend to attempt to resolve cybersecurity problems by increasing 'criminalisation' – i.e. arranging tightening the reins through criminal law – but this is not necessarily the best or only solution. The countries studied here also illustrate alternative routes to regulating the field.

2. The multi-stakeholder, private-public partnership approach is considered to be a crucial characteristic for governing cyberspace. All countries recognize this and this approach is evident in all the cases, albeit in slightly different forms. While there are considerable advantages to such an approach, the disadvantages highlighted here (such as coordination problems) should not be overlooked.

3. In light of point 2, in such arrangements, who is coordinating between stakeholders (including who takes the lead and who has ultimate responsibility) should be clear and formally delineated.

4. Policy makers can increase oversight efforts, which will indicate where there are potential gaps in both systems and the processes that govern them. Especially in differentiated forms of collaboration and cooperation, oversight is crucial.

5. In multi-stakeholder collaborations, especially where certain actions are based on voluntary efforts, trust is a key success factor. Trust cannot be demanded or regulated, but fostered through good communication, information exchange and making clear agreements regarding division of tasks and actions to be taken.

6. Cybersecurity is not necessarily separate from national security or civil protection, but an exceptional case that requires specific attention for the aforementioned points. Countries should carefully consider whether and how they regulate cybersecurity in relation to national security and civil protection: both an integrated governance regime and separate regimes can be employed, but either way, public policy should address the pitfalls in an integrated approach (e.g., too complex or too vague approaches, insufficient attention for the specifics of cybersecurity) or those in a separated approach (e.g., lack of coordination, policy competition, redundancy).

This comparative quick scan gives a broad overview of the governance arrangements for three cases in five countries. Delving further into the current structures and future plans requires more in-depth research, whereby limiting the number of countries is recommended. Given the rapid pace of developments in the field and the absence of a central authority to steer or coordinate the process in many situations, more discussion is needed on how far society wants to proceed in engaging the private sector in public security, what possible tensions may still arise in such an arrangement and how this can best be regulated.

1. Introduction

The increased dependency of society on networked technologies and infrastructures poses a new challenge to governments and other actors to ensure the sustainability and security of all things ‘cyber’. Cybersecurity is a particularly complex field, combining domains as diverse as information security, critical infrastructure protection, national security, cybercrime, cyber-terrorism and cyber-warfare. For such a complex field, the question of how cybersecurity can be effectively organised is particularly relevant to address. While the threats are real, in many cases, the debate that addresses them tends to focus on what *might* happen in the future,[1] whereby the nature and imminence of the threat, as well as how to resolve it, is not always immediately evident. As this report will further show, ensuring that the appropriate cybersecurity structures, processes and measures are in place and working is not only a responsibility and concern of the government, but is shared by and distributed among a wide variety of both public and private actors. It is here that the question of *governance* comes in: How are public-policy regulatory measures used to organise a process that involves (regulatory) actors outside of the government?[2]

Governance currently tends to be the result of a complex interaction of various actors, acting in different places and forums – a phenomenon that can be designated as polycentric governance. Because both cybersecurity structures and related cybersecurity policy are still in a relatively early stage of development, we do not as yet have a clear view what the landscape of cybersecurity governance looks like. The **aim** of this study is therefore to develop a better understanding of this landscape. This will be accomplished through a quick scan of current developments in cybersecurity policies, institutions, and regulation in several different countries.

The central **research question** is:

How is cybersecurity governance organised in a number of selected countries?

This question is addressed through the following **sub-questions**:[3]

1) What is cybersecurity?
2) Which actors are involved in cybersecurity, and how are the responsibilities for cybersecurity distributed among these?
3) How are the responsibilities for cybersecurity regulated by law and other forms of regulation?

[1] Dennis Broeders, *Investigating the place and role of the armed forces in Dutch cybersecurity governance* (Erasmus University Rotterdam 2014).

[2] Cf. Broeders 2014, p. 12 on ‘governance’.

[3] In the original proposal for this study, a fourth question regarding the application of mandatory security standards to information technology was included. This question is not addressed in this report, partly because it is a different type of question than the core issue researched in this report—how cybersecurity is *organised* (rather than specifically regulated)—and partly because this question is already addressed in a recent report, see T.F.E. Tjong Tjin Tai et al, *Duties of care and diligence against cybercrime* (Wolf Legal Publishers 2015).

1.1 Methods

In order to answer the central research question, we will use a comparative case-oriented policy and stakeholder analysis. Developments in public policy and political science research have repeatedly demonstrated the added value of using a comparative method, which enables one to analyse a multitude of relationships (combinations, patterns, interactions), account for irregularities and take into account detailed, but relevant, information.[4]

For this project, we have chosen to study five countries, as this is a sufficient number of countries to acquire an overview of the various ways that cybersecurity governance is, or can be, organised. The selection of countries should meet the following criteria: geographic diversity, different legal traditions, presence of a national cybersecurity strategy, a high ranking on the ICT Development Index,[5] and availability of sources. Based on these criteria, we have chosen the following countries: Canada, Estonia, Germany, the Netherlands, and the United Kingdom.

In order to flesh out how particular challenges in cybersecurity are organized in these different countries, we have selected three illustrative cases in cybersecurity governance. Focusing on cases allows us to acquire insight into sub-questions 2 and 3: the organization and regulation of cybersecurity, in a sufficiently contextualized manner. In order to enable sufficient focus in the analysis, each case zooms in on a concrete question how a particular challenge in cybersecurity governance is organized.

The three cases and concrete questions are:

- **Botnets**: how is botnet mitigation, both combating the infection of end-user computers with malware and combating denial-of-service attacks committed with botnets, organized?
- **Protection of vital infrastructures**: how is continuity of electricity provisioning, particularly the protection against cyber-attacks in the context of the transition towards smart grids, organized?
- **Identity infrastructures**: how is secure authentication of citizens in the context of e-government, in particular electronic service delivery, organized?

This selection was made on the basis of three criteria. First, since the landscape of cybersecurity governance is relatively unexplored, we chose cases that are diverse, rather than cases that all lie close to the core of cybersecurity (a maximum variation approach to case study research)[6], as this is likely to generate more insights into how cybersecurity is organized in the various countries. Second, the cases cover the main aspects of cybersecurity, namely confidentiality, integrity and availability. Because these three elements are inextricably intertwined, the cases are should not be viewed as a one-on-one match to these ideas, but rather as containing all three, yet reflective of different degrees in which the elements may be present, whereby one may be more dominant than the others. For example, confidentiality concerns are a primary aspect of botnet mitigation (but

[4] Robert H. Blank and Viola Burau, *Comparative Health Policy* (Palgrave, 2010).

[5] See International Telecommunications Union (ITU), *Measuring the Information Society Report 2014*, p. 42.

[6] Jo Segers and Jan Hutjes. *Methoden voor de Maatschappijwetenschappen* (van Gorcum, 1999).

availability is also important), whereas both authenticity and confidentiality are imperative to preserve the integrity of government-citizen relationships and availability is a key issue in relation to vital infrastructures. Third, the cases cover various forms of governance. In particular, we have looked at three *domains* in which the government classically plays an important role: law enforcement (with which botnet mitigation is primarily associated), national security (of which protection of vital infrastructures is traditionally an important part), and service delivery (of which a secure identity infrastructure is an important element). Within each of these domains, shifts are taking place towards involving private actors, and cases have been selected in which the involvement of private actors can be readily seen in current practices. The different extents and modalities of public-private interaction can thus provide interesting insights into how cybersecurity governance is or can be organized.

Sub-question 1, on the concept of cybersecurity, is answered through desk research, primarily of theoretical and analytical academic literature and policy reports on cybersecurity and governance. For answering the sub-questions 2 and 3, involving the three cases in the different countries, we rely primarily on desk research, using reports, academic literature, parliamentary record (legislative debate) and legislation and case-law. As part of this desk research, we also conducted a web search to ensure we had an overview of the relevant actors. The initial findings of the desk research were validated through interviews with eight country experts (see Appendix 1 for a list of interviewees).

1.2 Limitations

The research for this report was limited in time and resources, and therefore has the character of a quick scan. As a result, this report can only touch the surface of cybersecurity governance, which is an extremely complex (and dynamic) field. Both elements – cybersecurity and governance – are large and under-defined concepts and the combination cannot be explored in depth. As can be seen in the case-study approach, we do not aim to be comprehensive, and the cases are not necessarily generalisable towards other challenges in cybersecurity. Nevertheless, we hope that within the limited scope of this quick scan, the discussion of diverse cases in different countries illustrates the challenges of cybersecurity governance as well as how countries are addressing these challenges.

The research for the report was finalised in August 2015; the text of the report was finalised in October 2015. Developments after August 2015 have not been processed in the text.

1.3 Outline of the Report

In chapter 2, cybersecurity governance is analysed in order to acquire a firmer understanding of this complex and under-theorised term. Based on various perspectives, we develop a working definition of cybersecurity and cybersecurity governance, and provide some key theoretical insights into this concept. Chapters 3 through 5 present the results of the case studies. Chapter 3 outlines surveying how the selected countries are dealing with botnet mitigation. Chapter 4 examines the protection of vital infrastructures. Because most countries list multiple types of vital infrastructures, we focus in particular electricity provisioning in light of recent high profile cases of cyber-attacks. Chapter 5 examines the case of identity infrastructures, in particular the infrastructures currently in place or being developed to identify citizens in electronic citizen-government communications. These results are brought together in Chapter 6, with particular focus on how cybersecurity governance is organised and regulated. This chapter concludes the report with answers on the sub-questions and the overall research question.

2. The Concept of Cybersecurity Governance

2.1 Introduction

Cybersecurity governance contains two individual concepts, each of which is a fuzzy concept that can be interpreted differently, depending on the perspective from which it is approached. Combining two fuzzy concepts potentially yields an even fuzzier concept. In this chapter, we therefore endeavour first to conceptualise cybersecurity governance, in order to provide a background against which the overview of cybersecurity policy efforts and activities in the following chapters can be understood.

The term *cybersecurity* is becoming increasingly popular and more widely used, as states adopt and revise national cybersecurity strategies (NCSs) that lead to actions with numerous consequences, including financial ones, for a broad range of actors. At the same time, however, scholars, states and standardisation bodies use and define this term in very different ways. It is therefore necessary to develop a clear and sensible conceptual model of the term cybersecurity, especially for its use in a specific NCS. In order to develop a better understanding and working definition of the concept of cybersecurity for the purposes of this report, recent academic research on the issue of cybersecurity is examined, along with proposed definitions of the term and related terms (such as information security, computer and network security, infrastructure protection, cybersafety) by standardisation bodies and various states.

Subsequently, we briefly outline the theoretical discussion about the concept of *governance*, a concept that is also very broad and used differently in various contexts. Since literature on the concept of governance is more prevalent than literature on the concept of cybersecurity, we will limit ourselves here to sketching the basic elements of governance that are relevant for the purpose of this report, and refer the interested reader to the available theoretical literature on governance.[7]

We then combine the insights into both concepts to provide a working definition of the concept of *cybersecurity governance*, and we will briefly discuss some theoretical insights emerging from the literature that help understanding the complexity of cybersecurity governance, both in theoretic (conceptual) and in practical (policy measures) terms.

2.2 Cybersecurity

The debate on cybersecurity in a broader sense[8] originated in the United States of America (US) in the 1970s, emerging as a response to technological innovations and changing geopolitical conditions, especially after the Cold War.[9] The debate did not spread to other countries before the

[7] See, e.g., Rod AW Rhodes, *Understanding governance: policy networks, governance, reflexivity and accountability* (Open University Press 1997); Anne Mette Kjær, *Governance* (Polity 2004).

[8] Using different terms (e.g. computer security) with a different emphasis (e.g. on classified information).

[9] Lene Hansen and Helen Nissenbaum, 'Digital Disaster, Cyber Security, And The Copenhagen School' (2009) 53 International Studies Quarterly 1155, also Myriam Dunn Cavelty, 'The Militarisation Of Cyber Security As A Source Of Global Tension' in Daniel Möckli (ed) *Strategic Trends 2012: Key Developments in Global Affairs* (Center for Security Studies 2012).

late 1990s.[10] Initially the concern was with classified information residing in government information systems. However, as computer networks grew and spread into more and more aspects of everyday life, the focus changed. The term *cybersecurity* was first used by computer scientists in the early 1990s, denoting a series of insecurities related to networked computers with the focus shifting beyond a mere technical conception of *computer security* to the threats arising from digital technologies, which could have devastating societal effects – on national security and/or economic and social welfare of the entire nation.[11] The focus was on general vulnerabilities of the entire society. Cybersecurity, thus, advanced from the confined realm of technical experts into the political limelight. With events such as the discovery of the nuclear-industry sabotaging *Stuxnet* computer worm, numerous tales of cyber espionage by foreign states, the growing dependence on the "digital infrastructure" along with the sophistication of cybercriminals and the well-publicised activities of hacker collectives, the impression is created that cyber-attacks are becoming more frequent, more organised, more costly and altogether more dangerous. As a result, a growing number of countries consider cybersecurity to be one of their top security issues.[12] After 2010 the tone and intensity of the debate changed even further: the latest trend is to frame cybersecurity in strategic-military terms and to focus on countermeasures such as cyber-offence and cyber-defence, or cyber-deterrence.[13]

In current discussions on cybersecurity, there is a focus on critical infrastructures, due to an increasing dependence of societies on the smooth functioning of all sorts of computer-related applications, such as software-based control systems – a combination of vulnerabilities, technology and transnational interdependence. There is also an increased focus on states as the primary cyber "enemy", coining the term cyber-espionage (meaning high-level penetrations of government and business computer systems), as well as on increases in "hacktivism", a portmanteau combining hacking and activism and denoting a phenomenon of deliberately challenging the self-proclaimed power of states to keep information considered vital for national security secret (e.g. *Wikileaks*, hacker collectives such as *Anonymous* and *LulzSec*). There is also recognition for what may be described as a process of "cross-fertilization" of cyber-threats and terrorism, where cyber-threats support the claims to the dangerous nature of the terrorists and the terrorist character of the attacks makes them more worthy of attention.[14]

Against this background of the development of the concept of cybersecurity, in this section we attempt to analyse how the term 'cybersecurity' can be understood. There are various ways to define a term. In this section, we approach the concept of cybersecurity from different angles, in order to get a better grasp of the possible meaning(s) of the term. Starting with a grammatical approach, we dissect the term into its components ('cyber' and 'security'). We then apply a hermeneutic approach, understanding the concept by placing it in the context of related terms with

[10] Hansen and Nissenbaum 2009.

[11] Hansen and Nissenbaum 2009, Dunn Cavelty 2012.

[12] Dunn Cavelty 2012.

[13] Against the background of the Stuxnet incident; see Dunn Cavelty 2012.

[14] Dunn Cavelty 2012.

which it shares family resemblances, such as information security and cybersafety; discussing the commonalities and differences between related concepts is a good way to highlight the nuances of a term. Finally, we apply a pragmatist approach, identifying how the concept is used in practice by various stakeholders. Having explored the concept from these different angles, we develop a working definition of cybersecurity.

2.2.1 Grammatical approach: the constituent terms

Cyber

The term cyberspace literally means “navigable space” and is derived from the Greek word *kyber*, meaning to navigate. It was composed by fiction (*sci-fi*) writer William Gibson in his 1984 novel *Neuromancer*, where cyberspace refers to a navigable, digital space of networked computers accessible from computer consoles.[15] Since its introduction in *Neuromancer*, the term cyberspace has become widely used. It has, moreover, been re-appropriated, adapted and used in a variety of ways, all of which refer in some way to emerging computer-mediated communication and virtual reality technologies.[16]

“Cyberspace is geographically unlimited, non-physical space, in which – independent of time, distance and location – transactions take place between people, between computers and between people and computers. Characteristic of cyberspace is the impossibility to point to the precise place and time where an activity occurs or where information traffic happens to be.”[17] Cyberspace should not be equated with the technological components that constitute this space: apart from the technological layer, there is also a socio-technical layer in which cyber-activities take place, and this socio-technical layer is equally important to protect as the technology layer itself.[18]

Cyberspace today does not consist of one homogenous space; rather, it is a myriad of rapidly expanding cyberspaces, each providing a different form of digital interaction and communication. These spaces can be categorised into those existing within the technologies of the Internet, those within virtual reality[19] and conventional telecommunications such as the phone, and the hybrid spaces that emerge through the rapid convergence of these technologies.[20] In view of this, Dodge and Kitchin propose that the definition of cyberspace should focus on cyberspace as *conceptual space* within ICTs (information and communication technologies), rather than on technology itself.[21]

Certain states give their own definition of cyberspace in their NCSs. For example, Germany defines cyberspace as, “the virtual space of all IT systems linked at data level on a global scale.

[15] Martin Dodge and Rob Kitchin, *Mapping Cyberspace* (Routledge 2000), p.1.

[16] Dodge and Kitchin 2000, p.1.

[17] Cees J Hamelink, *The ethics of cyberspace* (Sage 2001), p. 9.

[18] Jan van den Berg and others, ‘On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education’ (NATO STO/IST-122 symposium, Tallinn, 13-14 October 2014), p. 12-2.

[19] Virtual reality technologies create visual, interactive computer-generated environments in which the user can move and explore (currently there are two forms of it: as a totally immersive environment and as screen-based).

[20] Dodge and Kitchin 2000, p.1.; also Hamelink 2001, p.9.

[21] In line with Gibson’s original definition; Dodge and Kitchin 2000, p.1.

The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace."[22] Such a definition, as is common, focuses on the Internet, although it does acknowledge other "virtual spaces of all IT systems". The 2009 UK NCS defined cyberspace as encompassing all forms of networked, digital activities, including the content of and actions conducted through digital networks. When the UK revised its NCS in 2011 it also revised its definition of cyberspace, which was then re-defined as, "an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the Internet, but also the other information systems that support our businesses, infrastructure and services. Digital networks already underpin the supply of electricity and water to our homes, help organise the delivery of food and other goods to shops, and act as an essential tool for businesses across the UK. And their reach is increasing as we connect our TVs, games consoles, and even domestic appliances." France defines cyberspace as, "the communication space created by the worldwide interconnection of automated digital data processing equipment" in its 2010 Information system defence and security document.

Security

Of the various meanings of security, the most important ones in the context of cybersecurity are:[23]

> 2. Freedom from danger or threat.
>
> a. The state or condition of being protected from or not exposed to danger; safety.
>
> b. The safety or safeguarding of (the interests of) a state (or, sometimes, a coalition of states) against some internal or external threat, now esp. terrorism, espionage, etc.; the condition of being so safeguarded.
>
> c. The condition or fact of being secure or unthreatened in a particular situation; freedom from material or financial want; stability, assurance (of rights, position, employment, etc.).
>
> d. The safety of an organization, establishment, or building from espionage, criminal activity, illegal entrance or escape, etc.
>
> e. With reference to encryption, or telecommunications or computer systems: the state of being protected from unauthorized access; freedom from the risk of being intercepted, decoded, tapped, etc. (…)
>
> 9. orig. *Mil.*
>
> a. Measures taken to safeguard the interests of a state or organization against threat; in early use *spec.* the maintenance of secrecy or cover. Hence more generally: any checks and procedures intended to keep a person, place, or thing secure and to prevent criminal activity,

[22] Germany's NCS from 2011.

[23] Oxford English Dictionary, entry 'security', http://www.oed.com (accessed 1 April 2015).

> illegal entrance or escape, etc.; (*concr.*) the area or place in which such checks are conducted. Cf. sense 2b.
>
> b. Sometimes with capital initial. A department responsible for guarding an organization against criminal activity, unauthorized access, etc. Also (orig. *U.S.*): the members of such a department collectively.

Security as it is used in the term 'cybersecurity' has connotations of many of these meanings: it is both the process (meaning 9) and the result (meaning 2) of taking measures to protect things, people, organisations, society, and the state itself. Security can thus be seen as a particular type of politics applicable to a wide range of issues – not only to the military and political context (traditional view) but also to the economic, environmental and societal context.[24] Whereas the military and state elements once primacy in the conceptualisation of security, since the 1970s the security agenda has widened, especially with the rise of economic and environmental agendas in international relations, concerns with identity issues and the rise of international crime.[25] The term security itself has a political function, demanding state action in a broad range of issues.

The general concept of security is at least partially drawn from the national security discourse – within that discourse it implies an emphasis on authority, the confronting and construction of threats and enemies, an ability to make decisions, and the adoption of emergency measures.[26] According to certain theoretical perspectives, security has a particular discursive and political force and is a concept that does something – it "securitizes" – rather than being an objective (or subjective) condition (see below). According to the perspective of the Copenhagen School's theory of securitization, security is, "the product of an historical, cultural, and deeply political legacy"[27] and is a discursive and political practice rather than a material condition or a verifiable fact. The "threat-danger-fear-uncertainty discourse" that the Copenhagen School defines as securitization is not universal, but "contextually and historically linked to shifting ontologies of uncertainty."[28] The understanding of security as a discursive modality with a particular rhetorical structure and political effect makes it particularly suited for a study of the formation and evolution of cybersecurity discourse.

2.2.2 Hermeneutic approach: related terms

Computer security

The Klimburg NATO National Cybersecurity framework states that computer security usually seeks to ensure the availability and correct operation of a computer system without concern for the

[24] Barry Buzan, Ole Waever, and Jaap de Wilde, *Security: A new framework for analysis* (Lynne Riener 1998); pp. vii, 1.

[25] Buzan, Waever and de Wilde 1998, p. 2.

[26] Hansen and Nissenbaum 2009.

[27] Michael C Williams, *Culture and Security: Symbolic Power and the Politics of International Security* (Routledge 2007), p. 17, as cited in Hansen and Nissenbaum 2009, p.1156.

[28] Niels Bubandt, 'Vernacular Security: The Politics of Feeling Safe in Global, National and Local Worlds' (2005) 36 Security Dialogue 275, p. 291, as cited in Hansen and Nissenbaum 2009, p.1172.

information stored or processed by the computer.[29] The history of cybersecurity began with the disciplines of computer and information science as computer security.[30] One use was in the Computer Science and Telecommunications Board's (CSTB) report from 1991,[31] which defined security' as, "protection against unwanted disclosure, modification, or destruction of data in a system and also [to] the safeguarding of systems themselves."[32] Security, in the sense of computer security, comprises both technical and human aspects;[33] it ''has significant procedural, administrative, physical facility, and personnel components.''[34] (CSTB 1991) Threats to cybersecurity, thus, not only arise from (usually) intentional agents, but also from systemic threats. Computer security, as used by the majority of computer scientists, adopts a technical discourse that is focused on developing good programs with a limited number of (serious) bugs and systems that are difficult to penetrate by outside attackers.

Information security

Information security 'is concerned with the protection of confidentiality, integrity, and availability of information in general, to serve the needs of the applicable information user'.[35] Although the term information security focuses on information, it should be observed that the focus of the security usually is data. The protection of information or data should be regardless of the form the data may take: electronic, print or other forms.

Information assurance

Information assurance is a superset of information security, and deals with the underlying principles of assessing what information should be protected. Even though the terms information security, computer security and information assurance address slightly different viewpoints, the terms are often used interchangeably.[36]

ICT security

ICT security is more directly associated with the technical origins of computer security, and is directly related to 'information security principles' including the confidentiality, integrity and availability of information resident on a particular computer system. ICT security, therefore, extends beyond devices that are connected to the Internet to include computer systems that are not connected to any network. At the same time, the use of the term ICT security usually excludes questions of illegal content, unless they directly damage the system in question, but it does include the term 'supply chain security'. The term "ICT security" substituted the term 'Application Security', which was defined as 'a process to apply controls and measurements to an organisation's

[29] Klimburg NATO, 'National cybersecurity framework manual' (2012).
[30] Hansen and Nissenbaum 2009.
[31] Computer Science Telecommunications Board (CSTB), 'Computers at Risk: Safe Computing in the Information Age' (National Academy Press, 1991).
[32] CSTB 1991, p. 2.
[33] Hansen and Nissenbaum 2009, p. 1160.
[34] CSTB 1991, p. 17.
[35] Klimburg NATO, 'National cybersecurity framework manual' (2012).
[36] Idem.

applications in order to manage the risk of using them. Controls and measurements may be applied to the application itself (its processes, components, software and results), to its data (configuration data, user data, organisation data), and to all technology processes and actors involved in the application's life circle.'[37] ICT threats arise from both software and hardware failures; since both software and hardware can never be made completely fool-proof in practice there is an inherent ontological insecurity within computer systems.[38] Complete ICT security can, thus, never be achieved and also should not be the goal of cybersecurity policy.

Network security

The Klimburg NATO National Cybersecurity framework states that network security is concerned with the design, implementation, and operation of networks for achieving the purposes of information security on networks within organisations, between organisations, and between organisations and users.[39]

Infrastructure protection

According to the Klimburg NATO National Cybersecurity framework, critical information infrastructure protection (CIIP) is concerned with protecting the systems that are provided or operated by critical infrastructure providers, such as energy, telecommunication, and water departments. CIIP, thus, ensures that those systems and networks are protected and resilient against information security risks, network security risks, Internet security risks, as well as Cybersecurity risks.[40] This term is connected to the terms 'critical infrastructures' and 'vital infrastructures,' which are also sometimes used interchangeably. Protecting critical or vital infrastructures usually focuses on securing the systems operating them, but they may have wider or other implications (e.g., protecting the water infrastructure against bio-hazards) outside of the sphere of critical information infrastructure protection or vital infrastructure system security.

Cybersafety

The Klimburg NATO National Cybersecurity framework defines cybersafety as, "the condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable."[41] Cybersafety can also be defined in a simpler manner as safety within the social structure of the Internet.[42] Safety, here, is a broader notion than security, involving not only the freedom from danger or threat through malfunctioning of cyberspace infrastructure or components, but also through undesirable content or content-related criminal activities, such as online grooming or hate speech. In this sense, cybersafety is a broader notion than cybersecurity.

[37] Idem.
[38] Hansen and Nissenbaum 2009.
[39] Klimburg NATO, 'National cybersecurity framework manual' (2012).
[40] Idem.
[41] Idem.
[42] Wouter Stol, *Cybersafety overwogen* (Boom Juridische Uitgevers 2010), p. 16.

Cyber-risk management

Cyber-risk management has been described as, "a type of risk management that – complementary to the technical focus of information security risk management in the technical layer – focuses on the risks the [sic] have emerged in the socio-technical layer of cyberspace. *Cyber risks* concern the IT-dependent risks all *cyberspace actors* in the various cyber dub-domains are exposed to when performing their above-mentioned cyber activities."[43] Cyber-risk management can be seen as an evolution of classical information or computer security, with an increasing incorporation of business-oriented concerns such as business continuity management,[44] and in that sense it can be used a synonym of cybersecurity.

2.2.3 Pragmatist approach: how the term is used

Following from state-specific definitions of cyberspace, related policy documents and NCSs provide some form of definition of the term cybersecurity. This section outlines three international definitions, followed by a selection of state-specific definitions (European countries only).

International definitions

a. Klimburg NATO (2012)

"'Cybersecurity', or 'cyberspace security' has been defined as the 'preservation of confidentiality, integrity and availability of information in the Cyberspace'. However, it has also been noted that other properties such as authenticity, accountability, non-repudiation and reliability can be involved in cybersecurity."[45]

b. International Telecommunication Union (2010)

Cybersecurity represents "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality."[46]

[43] Van den Berg et al. 2014, p. 12-3.

[44] Van den Berg et al. 2014, p. 12-2—12-3.

[45] Klimburg NATO, 'National cybersecurity framework manual' (2012), p. 10 (references omitted).

[46] ITU homepage: https://www.itu.int/net/itunews/issues/2010/09/20.aspx. This definition is also accepted in the ENISA, 'Cybersecurity cooperation: Defending the digital frontline' (2013) on NCSs in Europe. Available at: https://www.enisa.europa.eu/media/key-documents/cybersecurity-cooperation-defending-the-digital-frontline.

c. EU (2013)

The 2013 cybersecurity strategy for an open, safe and secure cyberspace defines cybersecurity in a footnote, stating that "cybersecurity commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."[47] It also introduces "principles of cybersecurity": (1) the EU's core values apply as much in the digital as in the physical world; (2) protection of fundamental rights, freedom of expression, personal data and privacy; (3) access for all; (4) democratic and efficient multi-stakeholder governance; (5) a shared responsibility to ensure security.

Selected national definitions

a. Austria (2013)

Austria's National ICT Security Strategy uses the broader concept of ICT Security and addresses cybersecurity and cyberdefence as vital and integral, but reactive strategies. However, neither cybersecurity nor cyberdefence can be applied effectively unless complemented by proactive strategy elements on a larger scale. The ICT Security Strategy is a proactive concept designed to protect cyberspace and human beings in this virtual space by taking into account their fundamental rights and freedoms. The country's specific approach to cybersecurity is closely linked to its existing stakeholders and structures, where cybersecurity refers to organisations, institutions or persons with a vested interest in, or particularly severely affected by, how it is defined.

b. Denmark (2013)

Denmark's NCS does not provide for a direct definition of cybersecurity. The NCS connects cybersecurity to cyberdefence. It states that with society's increased dependence on a properly functioning ICT infrastructure and an appropriate level of information security, there is an increased need for higher protection against cyberattacks. Also, military capacities are dependent on well-functioning ICT systems. The task of protection mainly falls under the Danish Ministry of Defence, needing to provide the capacity to execute both defensive and offensive military operations in cyberspace.

c. Estonia (2010)

The Estonian NCS contains a very broad national security concept, but refers specifically to cybersecurity, stating: "for ensuring cybersecurity it is essential to reduce the vulnerability of critical information systems and data communication connections and to contain possible damage from cyber attacks. Critical service information systems must be held operational throughout the entire

[47] European Commission, 'Cybersecurity Strategy of the European Union: An open, safe and secure cyberspace' (2013), p. 3. Available online: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

territory and on the basis of domestic resources, including in situations where connections with foreign countries are temporarily malfunctioning or have failed."

d. Finland (2013)

Finland's NCS defines cybersecurity as the desired end state in which the cyber domain is reliable and in which its functioning is ensured. In this desired state, the cyber domain will not jeopardise, harm or disturb the operation of functions dependent on electronic information (data) processing. Reliance on the cyber domain depends on its actors implementing appropriate and sufficient information security procedures, which can prevent the materialization of cyber threats, and, should they still materialize, prevent, mitigate or help tolerate their consequences. Cybersecurity encompasses the measures applied to the functions vital to society and the critical infrastructure that aim to achieve the capability of predictive management and, if necessary, tolerance of cyber threats and their effects that can cause significant harm or danger to Finland and its population. Cybersecurity is not meant to be a legal concept, the adoption of which would lead to granting new competences to authorities or other official bodies. In this respect no changes are proposed to the bases of contingency arrangements or to regulations concerning the competences of authorities.

e. France (2010, 2013)

Both the Information System Defence and Security Document (2010 and the White Paper on National Security (2013) centre on the notion of cyber defence, rather than cybersecurity. This is due to the recognition of cyber threats and development of cyber defence capabilities. The 2013 White paper notes the growing vulnerability of the state and society to increasingly dangerous attacks: attempts to penetrate networks for purposes of espionage, remote takeover, paralysis and, in the near future, destruction of infrastructures of vital importance, or even weapons systems and strategic military capabilities. The 2010 Information system defence and security document defines cyber defence as a set of all technical and non-technical measures allowing a State to defend in cyberspace information systems that it considers to be critical. In this document, cybersecurity is defined as the desired state of an information system, in which it can resist events from cyberspace likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible. Cybersecurity makes use of information systems' security techniques and is based on fighting cybercrime and establishing cyber defence. The 2010 document also states that in order for France to attain the primary goal of becoming a world power in cyber defence, cybersecurity of critical national infrastructures (among other things) needs to be strengthened and security in cyberspace needs to be ensured.

f. Germany (2011)

The German NCS distinguishes between civilian and military cybersecurity. Generally, cybersecurity is the desired objective of the IT security situation, in which the risks of cyberspace have been reduced to an acceptable minimum. Cybersecurity is the sum of suitable and appropriate measures. Civilian cybersecurity focuses on all IT systems for civilian use in German cyberspace. Military cybersecurity focuses on all IT systems for military use in German cyberspace. Germany's NCSs also makes clear that the protection of critical information infrastructures is the main priority of cybersecurity, since they are a central component of nearly all critical infrastructures and have become increasingly important. Another focus is on protection against cybercrime.

g. Hungary (2013)

According to Hungary's NCS, cybersecurity is the ongoing and planned application of political, legal, economic, educational, awareness-raising and technical tools capable of managing cyberspace risks, transforming the cyberspace into a reliable environment by ensuring an acceptable level of such risks for the smooth functioning and operation of social and economic processes.

h. Italy (2013)

Italy's National Cybersecurity Strategic Framework does not define cybersecurity. It states that the Framework and related National Plan aim at enhancing the national preparedness to respond to present and future challenges affecting cyberspace, and are devoted to directing all national efforts toward common and agreed solutions, knowing that cybersecurity is a process rather than an end to itself, that technical innovations will always introduce new vulnerabilities in the strategic and operational horizon, and that the intrinsic nature of the cyber threats makes our defense, at least for the time being, mostly – although not exclusively – reactive.

i. Netherlands (2013)

The Dutch NCS defines cybersecurity as "the effort to prevent damage due to disruption, failure or abuse of ICT and to restore damage in case it occurs".

j. Poland (2013)

Poland's NCS defines cyberspace security as a set of organizational and legal, technical, physical and educational projects aimed at ensuring the uninterrupted functioning of cyberspace.

k. Spain (2013)

Spain's NCS states that cybersecurity previously followed an information security approach, which only protected information against unauthorized access, use, disclosure, disruption, modification and destruction. Currently this approach is evolving towards cyberspace risk management (information assurance) where cybersecurity consists of the application of an analysis and management process for risks associated with use, processing, storage and transmission of information and data, as well as risks associated with the systems and processes used, based on internationally accepted standards. Cybersecurity should be formulated proactively as an ongoing process of analysis and management of risks associated with cyberspace.

2.2.4 A working definition of cybersecurity

Given the notion of cyberspace as an abstract term denoting the conceptual space constituted by computers and networks, cybersecurity can be seen as a comprehensive concept that builds on all the previous terms that focus on the security of particular components of cyberspace: computers, information, ICT, networks, and (ICT-based) infrastructures. Cybersecurity thus encompasses computer security, information security, ICT security, network security, and infrastructure protection. In line with the notion of information security, cybersecurity is concerned with the protection against threats to the confidentiality, integrity, and availability of information or data (and of the computers and networks in which data are processed); but it is not concerned with information as a threat in itself as such, i.e., with information that poses a risk *qua* information, such as hate speech or revenge porn. This distinguishes the concept from the broader notion of cybersafety, which also encompasses risks constituted by the informational content of the data processed within cyberspace.

Cybersecurity thus denotes the process and result of making cyberspace secure. Cyberspace in this context denotes a space that is constituted by information, ICT, networks, and (ICT-based) infrastructures. Although cyberspace is based on technological components, it is not identical to the technological layer itself; it denotes, rather, the conceptual space – facilitated by computer and networked technologies – that allows human and organisational activities to take place in a digital, interconnected environment. The security of this space consists of being free from threats to the confidentiality, integrity, or availability of the computers, networks, and information that together make up this space. Cyberspace itself, and the human and organisational activities using this space, should – as an ideal, not as a fully achievable goal – not suffer from malfunctioning of the infrastructure or any of its components, or from attacks on the infrastructure, its components, or the information processed using the infrastructure or its components. In short, cybersecurity can be defined as the proactive and reactive processes working toward the ideal of being free from threats to the confidentiality, integrity, or availability of the computers, networks, and information that form part of, and together constitute, cyberspace – the conceptual space that affords digitised and networked human and organisational activities.

2.3 Governance

Much like the terms discussed in the preceding section, the concept of governance has multiple definitions and can be used in various ways. When thinking about the term, it is therefore important to start with two basic distinctions: 1) government versus governance and 2) governance versus regulation. These distinctions already provide a route toward (partial) definitions of the term and at the same time point to some weaknesses of its use – and the related need for alternative (but still related) concepts.

2.3.1 Government versus governance

Traditionally, the governing authority at the centralized (nation-state) level was considered to have a monopoly on power not only in determining how a state was run, but also in defining which issues constituted the so-called public interest. In modern societies, however, non-governmental actors have played an increasing role in influencing policy outcomes, whereby the role of the centralized government (and, as such, its relationship to society) has changed. Most especially, changing dynamics in public-private relationships and influences at the systemic (international) level put the effectiveness and legitimacy of classical policy strategies and instruments up for discussion. In reignited academic debates about the role of governments, *governance* was (re-)introduced in the Political Science and Public Policy academic vernacular in an attempt to expand scholarly perspectives on politics and policy-making. Use of this term was intended to acknowledge that government is not the only (and may not even be the most important) actor in managing and organizing society and social processes.[48] Rather, in modern societies, the state increasingly finds itself in a mutually dependent triangle with the community and the market, all of which have particular (self-)regulatory processes that interact in complex ways. These three are thus dependant on one another and are increasingly affected by each other's unresolved problems.[49] In this respect, 'government' may be just one particular form of 'governance'.

The interdependent nature of the state-community-market relationship moved away from the traditional hierarchical structure where the state had the monopoly on power to a network structure involving new (types of) actors.[50] Moreover, government structures and authority were increasingly decentralized to localities. To reflect this, in the policy arena, a distinction is often made between horizontal and vertical relations. Horizontal refers to organizing the relevant public and private actors within a defined geographical or functional segment that play a role in steering society around a common aim, whereas vertical shows the links between them, such as institutional relations and balance of power.[51] It is important to note that at the nation-state level, it is not a question of whether the governance structure is horizontal or vertical; there is always a mix of central and local, hierarchical and networked, horizontal and vertical (this is sometimes referred to as polycentric governance).[52] To understand influences in the policy arena, it is therefore necessary to understand the interrelation between all elements. Broeders especially shows how crucial

[48] Marjolein van Asselt and Ortwin Renn, 'Risk Governance', (2011) 14 Journal of Risk Research 431, pp 431-449.

[49] Wolfgang Streeck and Philippe Schmitter, 'Community, market, state-and associations? The prospective contribution of interest governance to social order' (1985) 1 European Sociological Review 119, pp 119-138.

[50] See also Carolyn Hughes Tuohy, 'Agency, contract and governance: shifting shapes of accountability in the Health Care Arena' (2003), 28 Journal of Health Politics, Policies and Law 195, pp. 195-215.; Eelco van Hout, Kim Putters and Mirjan Oude Vrielink, 'Governance of local care and public service provision' (2007), Paper for the EGPA Conference in Madrid, September.

[51] See: Van Asselt and Renn 2011, p. 434; Broeders 2014, p.12.

[52] Van Hout et al. 2007.

public/private relations are in the cyberdomain and thus how new and emergent governance structures in the area of cybersecurity are both horizontal and vertical.[53]

2.3.2 Governance versus regulation

The shift in conceptual thought from government to governance and the related search for understanding emerging mechanisms of coordination between state and society raised questions regarding the new/changing role of regulatory mechanisms and subsequently led to attempts to distinguish between governance and regulation. While some authors still seem to define governance in more hierarchical terms, e.g. Colbridge et al. cite Jenkins when defining governance as prevailing patterns by which public power is exercised in a given social context [54] and van Hout et al (despite their description of moves to networks) discuss the influence of conduct to achieve goals, others frame governance in broader terms.

Van Asselt and Renn describe governance as, “the multitude of actors and processes that lead to collective binding decisions. Governing choices in modern societies is generally conceptualized as an interplay between governmental institutions, economic forces and civil society actors (such as NGOs),”[55] while Tuohy refers to governance in ‘loosely coupled networks.’ Tuohy further states, “this new governance paradigm is meant to connote the processes and instruments of governing in the context of complex organizational networks in which no one set of actors has authority to ‘command and control’”.[56] This last point is also seen as one hindrance to effective governance and will be discussed in the next section.

The best explanation regarding the distinction between governance and regulation is found in the work of Helderman et al: “Whereas ‘governance’ can be used for several different institutional orders (including spontaneous coordinated action) with multiple centers or networks, regulation is more restrictedly confined to the ‘sustained and focused control exercised by a public – independent – agency, over private activities that are socially valued.’”[57] Helderman et al further explain that the inclusion of socially valued activities in the definition distinguishes regulatory regimes from e.g. criminal justice systems and the reference to sustained/focused control implies that regulation is not just about law-making. It extends to include gathering information, monitoring performance and ensuring enforcement of established rules/standards. In other words, regulation is one distinct feature of how modern states steer society (including the economy) and while it is a significant feature, it is not the only mode. It is yet one of several possible examples of a strategy/process that may be employed to steer behaviours.

[53] Broeders 2014, pp 16 and 44.

[54] Stuart Corbridge, Glyn Williams, Manoj Srivastava and Rene Veron, *Seeing the State* (Cambridge University Press 2005); Rob Jenkins, ‘The Emergence of the governance agenda: sovereignty, neo-liberal bias and the politics of international development’ (2002) 1 The Companion to Development Studies.

[55] Van Asselt and Renn 2011, p 431.

[56] Tuohy 2003, p 202.

[57] Jan-Kees Helderman, Gwen Bevan and George France, ‘The rise of the regulatory state in healthcare: a comparative analysis of the Netherlands, England and Italy’ (2012), 7 Health Economics, Policy and Law 103, p 105, quoting Majone, 1994 in the second half of the definition.

What these definitions make clear is that governance reflects a transition in modern societies that expands the arena of actors and actions being taken, simultaneously restricting the capacity of the traditional authority (government of the nation-state to act). Governance refers to coordinating systems and their multiple actors and is underpinned by tensions between public/private (state and market) and between the centre and localities (different governmental levels).[58] Moreover, as van Asselt and Renn point out, the term governance often simultaneously contains both *descriptive* (observation and approach; who are the actors and what are the interactions between them?) and *normative* (an idealized model or framework for organizing and managing society) connotations. When discussing governance, the combination of actors, structures and processes, as well as the direct and indirect relations between them and ideas underlying their interactions, must be taken together.

2.3.3 Re-conceptualizing governance

While governance theory has moved scholars to think differently about the changing relationship between states and societies, governance itself remains a dynamic concept. Studying governance structures and processes empirically has revealed a number of practical issues that signify the need to refine what is meant by governance. Moreover, as modern societies progress and change, new challenges to these structures and processes arise (exemplified by the challenges of cybersecurity discussed in this report), also pointing to the need for more refined and specific concepts of governance in practice. Some authors have even suggested the need to move away from the typology of community-market-state, distinctions between public and private and notions such as hierarchy altogether, as these domains and the mechanisms at work within and between them are also in a state of flux.[59] Moreover, the changing relationship between government and social actors and is increasing the need for actors to be able to change roles in public and private environments,[60] which may lead to new types of social actors or *ad hoc* coalitions.[61] As such these authors have suggested using terms such as ‘multiple modes of governance’, ‘indirect governance’ and ‘co-governance’, which in many ways remain quite vague and fail to indicate how these apply to practical challenges.

First of all, the incorporation of multiple players interacting on multiple levels also implies multiple loci of responsibility and, as such, problems with ensuring accountability for enforcement.[62] There are limits to the technical capacity of government actors to define problems and understand what needs to be done in response, as well as to their institutional capacity of government to take action in response once the problem has been defined. Broeders’ reflection on the Internet as a particular challenge for governments is prime example of this. He shows the multi-centric nature of

[58] Blank and Burau 2010, p 69.
[59] See for example Taco Brandsen, Wim van de Donk and Kim Putters, ‘Griffins or Chameleons? Hybridity as a Permanent and Inevitable Characteristic of the Third Sector’ (2005) 28 International Journal of Public Administration 749, p 749-765; Tim Tenbensel, ‘Multiple modes of governance’ (2005) 7 Public Management Review 267, pp 267-288.
[60] Van Hout et al 2007.
[61] Van Asselt and Renn 2011.
[62] Tuohy 2003.

cybersecurity governance and the multiple agendas that come into play in attempting to identify problems and create common goals that lead to direct action. This is where the issue of command and control is once again raised. Sabel and Zeitlin argue that the combination of transnational connections and increased technological innovations have undermined the effectiveness of command and control. Where Broeders refers to the need to understand governance as "governance in progress," Sabel and Zeitlin offer a similar notion – "experimentalist" governance, which they define as a recursive process of provisional goal-setting and revision based on learning from the comparison of alternative approaches to advancing them in different contexts.[63] In its terminology the notion experimentalist also points to the sometimes trial-and-error nature of dealing with new challenges – and sometimes, finding creative solutions in the process.

The iterative, learning nature required of current governance structures and processes is related to a second practical challenge. The current issues confronting society are often ambiguous and complex – demanding a flexible response in the face of strategic uncertainty regarding what the nature of the problem is (and thus how best to approach it). This challenge has especially been highlighted in the area of scholarship devoted to theorizing so-called 'risk governance'. Risk governance tries to anticipate and respond to uncertainty regarding what *might* happen and what the consequences will be if it does. Whereas many discussions of governance implicitly seem to assume it is reactive ('as a response to changes in modern society…'), theories of risk governance and anticipation in the face of uncertainty show that governance structures and strategies must also often be proactive – which is where the coordinating mechanism aspect of the aforementioned definitions comes in.

The nature of many risks requires cooperation, coordination, trust and mutual understanding between a range of (types of) stakeholders, who often have not only diverging interests and but also contrasting perceptions of potential risks involved, whereby the various actors (including governments) have difficulty making decisions with confidence and legitimacy.[64] Moreover, they must act not just to minimize risk, but also to establish resilient systems that decrease general vulnerability to unanticipated events over a longer term. Similar to the idea of experimentalist governance, dealing with perceived risks often requires learning by doing (trial and error) and seeking creative solutions. Translated to the case of cybersecurity, minimizing risks to systems and establishing longer-term resilience within systems is a particular challenge. Inherent to risk governance is difficulty in pinpointing the source of (and, thus, the concrete solution to) a problem. As Broeders clearly shows, responses to threats are often demanded in situations where there is not a clear analysis of the actual problem, which can lead to e.g. alarmism and over-inflated threats.[65]

[63] Charles F. Sabel and Jonathan Zeitlin, 'Experimentalist Governance' in David Levi-Faur (ed), *The Oxford Handbook of Governance* (Oxford University Press, 2012).
[64] Van Assel and Renn 2011.
[65] Broeders 2014, pp 7-11.

Finally, the legitimacy issues that accompany the introduction of new actors, action under uncertainty and the sometimes creative solutions that emerge from this combination have also led to a rise in demand for reflection on the policies and strategies that are adopted and enacted. In addition to the iterative learning process discussed by Sabel and Zeitlen, Corbridge et al point to the importance of paying attention not just to notions of governance, but to notions of what constitutes *good* governance[66] (in accordance with social understandings of what constitutes 'right and wrong') and how these policies and strategies are assessed. Although agendas of good governance (and the very idea) themselves may be open to critique, the primary concern from a practical perspective is ensuring the balance between individual representation and the various actors involved in governing specific situations.

Whereas much of the impetus behind shoring up cybersecurity infrastructures in many cases seems to be premised on the idea of increased criminalization of threats to or occurring via networked technologies, this review of governance literature shows that governance is not only about command-and-control regulation to prevent 'bad' behaviour. Rather, it is about how various parties coordinate (or are coordinated in) anticipation of (and working responses to) potential threats, while at the same time developing and implementing longer term structures and processes that reduce ambiguity, uncertainty and the immediacy of threats from unanticipated events. Governance is thus about proactive and reactive approaches to social steering that strike a balance between multiple interests from various types of stakeholders and the overall steering of social processes in a politically legitimate manner (i.e., that has legitimacy in the eyes of individual citizens).

With regard to cybersecurity, key notions are the ambiguity and uncertainty with regard to threats and their potential solutions. This means that the issue of how the network infrastructure is conceptualized is important, because different conceptualizations can lead to different questions.[67] Moreover, how coordination mechanisms are used to ensure that the parties that must work together do so with confidence and trust is crucial.

2.4 Conclusion

Based on the above literature review, we develop the following working definition: cybersecurity governance refers to the approaches used by multiple stakeholders to identify, frame and coordinate proactive and reactive responses to potential threats to the confidentiality, integrity, or availability of the computers, networks, and information that together constitute cyberspace (the conceptual space that affords digitised and networked human and organisational activities). This includes not only short-term and concrete approaches to address known threats, but particularly also the development and implementation of structures and processes to reduce uncertainty and to enable to respond to threats from unanticipated events over the longer term. Hereby it is

[66] Corbridge et al. 2005, p. 152.

[67] Broeders 2014, p 44.

important to keep in mind that cybersecurity involves not only protecting the technology itself, but also the activities taking place in or facilitated by cyberspace. As such, how problems are identified, defined and framed within a given culture or setting is crucial.

3. Case 1: Botnet Mitigation

3.1 Introduction

Botnets are collections of compromised machines infected by bots – pieces of advanced malicious software that install system backdoors that connect back to remote machines via common communication channels. Every botnet has bot-masters (a.k.a. bot-herders), the actual agents in control of the common communication channels and thus capable of manipulating the infected machines. The power acquired by bot-masters is reflected in the size and resilience of the botnet, which can be used to perform further criminal acts. As a result, botnets can be very lucrative, as they generate income to their masters via a multitude of cybercrimes, i.e. data copying, extortion demands through DDoS attacks and ransomware, spam, search engine poisoning, and click fraud.[68] Mostly, infected users are unaware of their condition, as there may be no clear sign the device is contaminated. Moreover, botnets have grown to become complex, resilient infections, remaining under the radar of security tools such as firewalls and anti-viruses.

Recent industry reports revealed botnet infections affect 500 million computers every year, at a rate of 18 victims per second.[69] While statistics seem to vary and industry reports should be read cautiously (since security companies may have an interest in presenting high threat levels), a consensus exists that botnets are among the most serious threats to information security. A contemporary botnet trend is to exploit darknet, a collection of non-indexed domains, which makes authorship attribution a greater challenge. Darknet domains cannot be detected through regular internet search, since they are protected by multi-layered structures known as The Onion Router (TOR).[70] In addition, TOR enables anonymous internet communication between users, protecting their identities.[71] As a result, botnets operating in darknet domains present increased obstacles for law enforcement.

A typical botnet is developed through a lifecycle of multiple, connected stages: Conception; Recruitment; Interaction; Marketing; Execution and Success.[72] Therefore, any attempt to mitigate botnets must target and stop at least one of phases of the botnet lifecycle. In fact, by hindering the completion of any of these stages, the botnet success will be frustrated.[73] Ideally, however, botnet mitigation should occur as early as possible, starting in the recruitment or contamination phase, preventing malware from effectively infecting targeted machines. In practice, however, most botnet countermeasures only occur after the success of the operation has gained notoriety and/or caused significant costs to business and society.

[68] Alvaro A Cardenes et al., 'An Economic Map of Cybercrime' (Working Paper 2009). Retrieved from http://chess.eecs.berkeley.edu/pubs/772/cardenas_2009.pdf

[69] http://www.fbi.gov/news/testimony/taking-down-botnets

[70] Marie-Helen Maras, 'Inside Darknet: the takedown of Silk Road' (2014) 98 Criminal Justice Matters 22, p. 22.

[71] Maras 2014, p. 22.

[72] RA Rodriguez-Gomez, G Macia-Fernandez, and P Garcia-Teodoro, 'Survey and Taxonomy of Botnet Research through Life-cycle' (2012) ACM Computing Surveys. Retrieved from http://wdb.ugr.es/~rodgom/wp-content/uploads/Survey.pdf

[73] Rodriguez-Gomez, Macia Fernandez, and Garcia Teodoro 2012.

3.2 Mitigation

Mitigation efforts may refer to different initiatives in different areas of society to minimise the threat posed by botnets. The European Union Agency for Network and Information Security (ENISA) calls identifies three specific approaches to fighting botnets: 1. Preventing new infections; 2. Mitigating existing botnets; and 3. Minimising criminal profit.[74] Any activity aiming at improving resilience against cybercrime, including prevention of new infections, mitigation of existing botnets, and efforts to minimise the profit of these criminal attacks, contributes to botnet mitigation at large. Each of these steps requires a multifaceted approach to deterrence and prevention: detection and mitigation of botnets requires efforts beyond the technical level, and must include measures targeting public policy, social awareness and training, legislation, and economics of cybercrime.

In this context, botnet takedowns are important means to interrupt on-going botnet activity. A takedown, in the very sense of the term, brings down the botnet by disrupting the common communication channel that determines the behaviour of the infected machines. Another form of disrupting a botnet is through takeovers, by which an external agent takes control of the central servers and injects code to block the communications with the malicious centres, to redirect infected machines to a white server, or to remotely disinfect all zombies and therewith liberate machines from the poisonous network. One important element of botnet disruption is the involvement of private sector agents, especially the participation of ISPs, which are often in a better position to collect information about the attacker and identify infected machines. Yet, it is not clear how far ISPs can go in cooperating with public authorities, in particular law enforcement, in the context of disruption. On the one hand, ISPs have the overarching right to secure their networks, their reputation, and to protect their customer, what could legitimise the launch of countermeasures from their side. On the other hand, it is not clear how these activities could be compatible with the right to privacy of users, as the collection of intelligence data about botnets often involved gathering of personal data flowing in the zombie machines. Finally, ISPs face liability issues in the event of false positive or unintended consequences following countermeasures, making the decision of launching countermeasures even more daunting.

It follows from the above that takeovers and takedowns are time-consuming and require large resources, as well as a solid network of public and private sector agents cooperating with one another. Therefore, a holistic front against botnets must involve coordinated actions in different areas of computer security. This report focuses on legislation and organisational structures dealing with botnets and cybercrime mitigation in relation to the three areas suggested by ENISA.

3.2.1 Preventing new infections

Important steps in preventing new infections include patching existing vulnerabilities and fostering a culture of security-by-design. By patching infections, exposed vulnerabilities are shielded from contamination, or immunized against new exploitation. Fixing non-zero-day exploits is paramount

[74] Jan Gassen, Elmar Gerhards-Padilla, and Peter Martini, 'Botnets: How to Fight the Ever-Growing Threat on a Technical Level' in Heli Tirmaa-Klaar et al., *Botnets* (Springer 2013).

in thwarting many forms of botnets whose modus operandi are already known to developers. In addition, a culture of security-by-design involves investment in awareness, capacity building, and training, and has long been promoted as an efficient way to empower users in keeping devices free from contamination. Fostering a cybersecurity mind-set among stakeholders would provide incentives for developers and manufacturers to be attentive to all security matters even before the product or service is placed on the market and empower users to protect themselves against botnet infections.

3.2.2 Mitigating existing botnets

Disrupting widespread, notorious botnets is key in botnet fighting. While security specialists have developed powerful technical solutions to tackle botnets (P2P polluting, PeerShark, Sinkholing, Sybil attacks, Crawling, among others), the preparation, resources, and costs associated with large operations are often prohibitive when not supported by law enforcement and State authorities. Additionally, effective botnet mitigation tools can be highly invasive, cause collateral damages, and raise ethical and legal issues. To that end, there is a need to invest in legal research exploring the use of anti-botnet solution. Likewise, mitigating existing botnets also includes disinfection of currently infected machines, which can be achieved by remote disinfection and awareness-raising campaigns aimed at diagnosis and disinfection by end-users. By enabling an efficient legal framework and supporting private sector participation and innovation in this area, public authorities can deliver important results, and prevent market failures from dictating security standards. Botnet mitigation, from a legal perspective, involves important discussions on fine-tuning international cooperation models and law enforcement powers, while safeguarding individuals' fundamental rights.

3.2.3 Minimising criminal profit

As long as botnets remain a profitable business, criminals will invest in circumventing security measures and find a way through them. Evidently, the economics of botnets depends on their modus operandi – every design has its own weaknesses. Increasing the costs of botnets in a given jurisdiction means enhancing prevention to the point that the effort to create and operate a botnet infrastructure is no longer interesting, and even when machines are infected, disruption is quick and effective. Moreover, increasing the costs of botnets in a given sector or jurisdiction may have only local effects. Criminal organisations targeting a specific company will shift to other same sector companies, if the costs of cybercrime became unattractive from the outset. Lastly, if a given jurisdiction makes cybercrime harder to generate income, botnets will migrate to countries that are more profitable. Ideally, countries should work together to provide a minimum level of prevention and deterrence against botnets worldwide, preventing the creation of cybercrime havens.

3.3 Case Study Countries

The following sections describe the approaches adopted in the case study countries, which includes both the legal and organisational measures and the distribution of responsibilities between different sectors and agents. The cases are discussed in the following order: Canada, Estonia, Germany, the Netherlands and the UK.

3.3.1 Canada

The Canadian Cyber Security Strategy,[75] launched in 2010, included a five-year action plan (2010-2015), built on three pillars: helping citizens be secure online, securing government systems and partnering to secure vital cyber systems outside the Federal Government. Since 2010, the Canadian Government recognises the need for collaboration with stakeholders, especially internationally, as an essential step into security. Public Safety Canada, the government department responsible for protecting Canadians and helping to maintain a peaceful and safe society, is responsible for coordinating the implementation of the Strategy together with private sector and international partners. In 2014, the Royal Canadian Mounted Police launched a Cybercrime Report with a specific section dedicated to botnets. The overall cyber security policy highlights the importance of shared responsibilities in ensuring security and the need to enforce collaboration across sectors, industry, and government.

CERTs

The Canadian Cyber Incident Response Centre (CCIRC) is the national Computer Emergency Response Team (CERT) of Canada, with the mandate of the federal government, to build safe and resilient internet in the country.[76] CCIRC acts as the national coordination centre for prevention and mitigation of attacks, as well as preparedness, response and recovery, providing authoritative support and advice, and coordinating information sharing among key partners. CCIRC collaborates with partners from public and private sectors, as well as international partners, producing information and distributing data that can improve cyber security. In case of infections, CCIRC notifies users of compromised systems on the nature of the contamination and on the steps for immunization. Besides, it shares best practices and guides with security tips and advices to mitigate malicious events CCIRC provides its partners with technical assistance, performing malware analysis and computer forensics. CCIRC partners include government, public and private sector organizations, security researchers and the national cyber security incident response teams (CSIRTs) of other countries. The community of partners working together with CCIRC have resulted in the creation of a CCIRC Community Portal, which provides tools and recent documents against threats. CCIRC was involved in the activities that led to the disruption of Gameover Zeus and Cryptolocker in 2014.[77]

[75] Available at http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf
[76] See http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx
[77] See http://news.gc.ca/web/article-en.do?nid=852959

Applicable framework

Criminal offences

The Canadian Criminal Code, combined with special legislation, is the main source of substantive criminal law in the country. Under Section 342.1(1) of the Canadian Criminal Code it is an offence to fraudulently and without right obtain any computer service, use (or cause to be used) a computer system with the intent to commit an offence in relation to computer data and to computer system, and to use, possess, traffic in or allow another person to have access to a computer password that would enable a person to commit an offence, as well as to intercept or cause to be intercepted any function of a computer system. The offence of Section 342.1 (Unauthorized access) is broad to cover hacking in the context of botnets. Additionally, Section 342.2 criminalises the unlawful making, possession, selling, offering for sale or distribution of any instrument or device or any component thereof designed to commit any offence under Section 342.1 or which renders it primarily useful for such offences. Section 342.2 thus criminalises a wide range of activities connected to handling of malicious codes, which is utmost relevant for criminalising bots. Data interference such as DDoS attacks are covered by Section 430(1.1) – Mischief of computer data – which defines as an offence, among others, to obstruct, interrupt or interfere with the lawful use of computer data, to obstruct, interrupt or interfere with a person in the lawful use of computer data or to deny access to computer data to a person who is entitled it.

Investigatory powers

On July 8, 2015, Canada ratified the Council of Europe Convention on Cybercrime. According to Canadian authorities, the 2014 Protecting Canadians from Online Crime Act[78] (which criminalises cyberbullying and widens investigative powers "to help police and prosecutors investigate not only the proposed new offence, but other existing offences that are committed via the Internet or that involve electronic evidence"[79]) already provided the necessary means for police to duly investigate cybercrime, fulfilling the requirements for ratification.[80] The summary of the Protecting Canadians from Online Crime Act describes the new powers as: "... (b) the power to make preservation demands and orders to compel the preservation of electronic evidence; (c) new production orders to compel the production of data relating to the transmission of communications and the location of transactions, individuals or things; (d) a warrant that will extend the current investigative power for data associated with telephones to transmission data relating to all means of telecommunications; (e) warrants that will enable the tracking of transactions, individuals and things and that are subject to legal thresholds appropriate to the interests at stake; and (f) a streamlined process of obtaining warrants and orders related to an authorization to intercept private communications by ensuring that those warrants and orders can be issued by a judge and by specifying that all documents relating to a request for a related warrant or order are automatically subject to the same rules

[78] S.C. 2014, c. 31, Assented to 2014-12-09, available at: http://laws-lois.justice.gc.ca/eng/annualstatutes/2014_31/FullText.html

[79] Myths and Facts Bill C-13, Protecting Canadians from Online Crime Act. Available at: http://news.gc.ca/web/article-en.do?nid=832399

[80] See http://www.international.gc.ca/media/aff/news-communiques/2015/07/08b.aspx?lang=eng

respecting confidentiality as the request for authorization."[81] These powers can also be used for executing incoming requests for mutual legal assistance in criminal matters.

The Cybercrime Convention will enter into force exactly three months after the ratification is officially communicated to the Secretariat of the COE. Currently, the Canadian Criminal Code, combined with special legislation, is the main sources of criminal procedure rules in Canada. The production order (Art. 18 Cybercrime Convention) is regulated in Section 487.014 et seq. Criminal Code, whereby law enforcement can request data about a subscriber or traffic data from a telecommunication operator. This provision finds a parallel in Section 7(3)(c.1) of the Personal Information Protection and Electronic Documents Act, which allows data controllers to disclose personal data, such as name, IP address, email, and telephone number to law enforcement,[82] without user knowledge or consent. Search and seizure of networks, as well as interception of communications data, form the concept of lawful access powers given to Canadian law enforcement, as provided in the Criminal Code and special acts, comparable to Arts. 19 (search and seizure of stored computer data); Art. 20 (collection of traffic data); and Art. 21 (interception of content data) of the Cybercrime Convention. All powers are subject to compliance with national privacy laws and the Canadian Charter of Rights and Freedoms.[83] These powers give law enforcement the possibility to intercept, search and seize or copy documentation, computer data, and other relevant evidence.[84] A bill to expand the scope and possibilities of lawful access in the context of cybercrime (Bill C-30),[85] proposed in 2012 with the purpose of amending the Criminal Code, died in parliament.[86]

Mitigation efforts

Canada has been involved in international efforts tacking botnets worldwide, such as the MDUS led initiative to takedown Gameover Zeus and Cryptolocker[87] and the Operation Clean Slate that targeted Citadel. In the latter, the Royal Canadian Mounted Police seized more than 80 physical servers connected to Citadel, in support to the activities initiated by the FBI.[88] Finally, Canadian stakeholders have worked together under the guidance of the European Cyber Crime Centre (EC3) in coordinated international efforts against cybercrime. The expectation is that the ratification of the Cybercrime Convention will intensify the cooperative efforts between Canadian law enforcement and other countries parties to the convention.

[81] S.C. 2014, c. 31.

[82] Library of Parliament, 'Cybercrime: issues' (Background paper, Publication no. 2011-36-E, 2011), p. 4. Available at: http://www.parl.gc.ca/content/lop/researchpublications/2011-36-e.pdf

[83] Available at: http://www.justice.gc.ca/eng/cons/la-al/sum-res/faq.html

[84] In 2014, the Supreme Court of Canada issued its decision in R. v. Spencer, strongly questioning the constitutionality of the police obtaining without warrant and voluntarily access to a subscriber's data held by an ISP.

[85] See http://www.parl.gc.ca/Content/LOP/LegislativeSummaries/41/1/c30-e.pdf

[86] See https://openparliament.ca/bills/41-1/C-30/

[87] Available at http://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware

[88] Royal Canadian Mounted Police, 'Cybercrime: an overview of incidents and issues in Canada' (2014), p. 9. Available at: http://www.rcmp-grc.gc.ca/pubs/cc-report-rapport-cc-eng.pdf

Multistakeholder initiatives

No particular multistakeholder initiative in Canada dealing with botnets was identified during this quick scan. It is important to note that multistakeholder initiatives often operate within sectors, where there is no clear interest for making this information available to the general public. Other multistakeholder initiatives in general areas of cybersecurity and crime include: 1. the activities led by Public Safety Canada with private sector agents; 2. the Canadian Telecommunications Cyber Protection Working Group, which promotes multiples partnerships between private and public sector in protecting Canadian networks; and 3. the Network for Security Information Exchange, which promotes collaboration between a larger community of cyber security stakeholders such as the telecommunications, financial, energy, and vendor communities and other government departments.

3.3.2 Estonia

The Cyber Security Strategy 2014-2017 (the Strategy) adopted by the Ministry of Economic Affairs and Communications of Estonia (MEAC) sets out the goal to increase cybersecurity capabilities and raise the population's awareness of cyber threats, thereby ensuring continued confidence is cyberspace. [89] MEAC is responsible for the security of state information systems, e-services and critical infrastructures and the overall policy coordination of cyber security.[90] The Strategy does not make explicit references to the need to fight or mitigate risks arising from botnets. However, the Strategy emphasizes that cybercrime is a general threat to the overall growing tendency of dependence of technology, use of government e-solutions and trust in cyberspace.[91] Also, the Strategy stresses the need for meaningful and effective cooperation between public and private actors in the development of cyber security organisation as well as in preventing and resolving cyber incidents that are becoming increasingly unavoidable.[92]

The Ministry of Justice (MJ), responsible for fighting and combating cyber-crime, has prepared a document "Criminal Policy Trends up to 2018" which noticeably lists prevention and effective reaction to cybercrime as a top priority in the field of criminal law.[93] The document sets out that the fight against cybercrime must focus on, *inter alia*, the prevention of computer-related fraud and the spread of computer viruses and hacking.[94]

[89] Ministry of Economic Affairs and Communications, 'Cyber Security Strategy 2014-2017' (2014), p 4 and 8. Available at https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

[90] In fact, these responsibilities are delegated to the Estonian Information Systems Authority (ISA) which is a subunit of MEAC. ISA is responsible for the development and administration of state information systems, drafting related policies and strategies, coordinating the implementation of security standards, manages the security incidents occurring in Estonian networks.

[91] According to the CCDCOE study National Cyber Security Organisation: Estonia, 94% of Estonians submit their income tax return via e-Tax Board and more than 90% of the residents of Estonia use the ID card that enables electronic authentication when using online services and vote online. E-voting has been used for local and parliamentary elections in Estonia eight times since 2005 (http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics). Available at https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_ESTONIA_032015.pdf.

[92] Cyber Security Strategy 2014-2017, p 5.

[93] Ministry of Justice, 'Criminal Policy Trends up to 2018' (2010), p 1. Available at http://www.just.ee/sites/www.just.ee/files/elfinder/article_files/kriminaalpoliitika_arengusuunad_aastani_2018.pdf.

[94] Ibid, p 3.

CERT-EE

As a subunit of Information System Authority (ISA), CERT-EE was established in 2006. It works as the governmental body responsible for assisting Estonian Internet users in the implementation of preventive and response measures. CERT-EE deals with security incidents that occur in Estonian networks or reported as such by citizens or institutions in Estonia or abroad. CERT-EE's incident response procedure is described as follows in the RFC 2350 of CERT-EE: a) incident triage: investigating whether an incident has indeed occurred and determining the extent thereof; b) incident coordination: contacting and determining relevant involved organizations; facilitating contacts and asking and composing reports; communicating with media, if necessary; c) incident resolution: advising involved organisations, following up the incident solution process, collecting evidence and interpreting data.[95] CERT-EE is affiliated with FIRST (the global Forum of Incident Response and Security Teams) as well as European regional forums TERENA (Trans-European Research and Education Networking Association), TF-CSIRT and TI (Trusted Introducer for European CERTs). CERT maintains affiliations with various CSIRTs around the world as needed.[96]

Applicable Framework

The Estonian Penal Code together with the Electronic Communications Act and the Code of Criminal Procedure are the main sources of law in regards to prevention, mitigation and apprehension of cyber-criminals.

Criminal Offences

Because the basis of the bot is hacking or 'electronic break-in,' section 217 of the Penal Code criminalises the act of illegally obtaining access to a computer system which is punishable up to three years' imprisonment. If aggravating circumstances exist (e.g. access was obtained to a state secret), the crime is punished with up to five years of imprisonment.[97] A serious shortcoming of section 217 is that it does not criminalise the act of obtaining illegal access to a part of the computer system.[98] Therefore, if an insider (e.g. an employee) has access to one part of a computer system and then illegally obtains access to another part that he or she had no authorisation to access, then the insider does not infringe section 217 of the Penal Code.

Once access to a computer system is obtained, a botmaster's further activities could fall under section 206, 207 or 406 of the Penal Code. Section 206 criminalises the act of interference[99] of computer data which is punishable by up to three years of imprisonment. If the act is committed against data in numerous computer systems, and if the perpetrator committed the act by using a

[95] See https://www.ria.ee/public/CERT/CERT-EE_rfc2350.pdf.
[96] Ibid.
[97] According to the study by the Ministry of Justice, there were 22 registered "hacking" cases in 2014. The study is available at http://www.kriminaalpoliitika.ee/sites/www.kriminaalpoliitika.ee/files/elfinder/dokumendid/kuritegevuse_at_2015_0.pdf.
[98] E Hirsnik, 'Arvutikuritegevuse regulatsioon Eestis: karistusõiguse revisjoniga toimunud muudatused ja lahendamata jäänud probleemid' (2014) VIII Juridica, p 613. Available at http://www.juridica.ee/juridica_et.php?document=et/articles/2014/8/244874.SUM.php.
[99] I.e. illegal alteration, deletion, damaging or blocking of data in a computer system.

device or a computer program that was created or adjusted in particular for the commission of the cyber-crimes, then the act is punishable with up to five years of imprisonment. According to the explanatory notes of subsection 206(2)(1), this is a botnet specific provision.[100]

Section 207 of the Penal Code criminalises the act of hindering the functioning of a computer system that must be seen as an extension of the aforementioned section 206 of the Penal Code[101] – if the act of illegal interference of data also hinders the functioning of a computer system, the act should be qualified as an act under section 207. This section criminalises the DoS attacks.[102] The Harju County Court (court of first instance in Tallinn) made a judgement regarding a DoS attack made during the events of the Bronze Night in 2007.[103] The DoS attack was made by a sophomore student against the website and intranet of the leading centre-right political party *Reformierakond*. The student was found guilty and had to pay a pecuniary punishment of EUR 1090.[104] In 2014, there were 9 registered infringements of section 207.[105]

In case the botmaster targets a vital service or a vital public utility system (e.g. a structure or a device of the energy, communication, signalling, water supply or sewerage system or traffic control) and as a result it causes interference with or interruption of the functioning of a vital public utilities system, section 406 of the Penal Code punishes the act up to five years' imprisonment.[106] The Penal Code also criminalises the act of preparation of a cybercrime. There were 37 of such registered incidents in 2014.[107]

Investigatory Powers

The Code of Criminal Procedure enables the police officer and the officer of the Internal Security Service covert access to the computer system to conduct surveillance if it is unavoidably necessary for the achievement of the objectives of the surveillance activities.[108] The Prosecutor's Office directs pre-trial proceedings and ensures the legality and efficiency thereof; also, it represents public prosecution in the court.[109] The Prosecutor's Office may issue orders to investigative bodies in order to meet the aim set out above.[110] In the context of botnets, the Police and Border Guard

[100] Added to the Penal Code on 1 January 2015.
[101] Hirsnik 2014, p. 613.
[102] According to the report of ISA regarding cyber security in 2014 (See https://www.ria.ee/public/Kuberturvalisus/RIA-Kyberturbe-aruanne-2014.pdf), there were 22 DoS attacks in Estonian networks in 2014. The report shows that this number has increased – in 2013, there were 13 DoS attacks. Sadly, the provision itself does not carry out the expectations it has been set – the sanction under section 207 is exactly the same as under section 206 – up to three years of imprisonment and up to five years if aggravating circumstances exist.
[103] See http://en.wikipedia.org/wiki/Bronze_Night.
[104] Judgement of the Harju County Court, 13 December 2007, court case number 1-07-15185. Available at https://www.riigiteataja.ee/kohtuteave/maa_ringkonna_kohtulahendid/download.html?fail=2008%5c1%5cCWLDXDHSYXHACMCALHMSYZQHNHZQDSST.pdf&viideFailile=1-07-15185.pdf.
[105] Crime in Estonia, Annex I, p 86.
[106] In 2014, there were 4 of reported section 406 infringements, however, the statistics do not reflect if any of those could be qualified as cyber-attacks.
[107] Crime in Estonia, Annex I, p 87.
[108] Section 126^3(5) of the Code of Criminal Procedure:
(5) Covert entry into a building, premises, vehicle, enclosed area or computer system is permitted upon conduct of the surveillance activities specified in subsection (1) and clauses (2) 2) and 3) of this section in the case this is unavoidably necessary for the achievement of the objectives of the surveillance activities.
[109] Subsection 30(1) of the Code of Criminal Procedure.
[110] Subsection 213(1)(5) of the Code of Criminal Procedure.

Board (the Police) and the Estonian Internal Security Service are investigative bodies who conduct pre-trial proceedings and may perform the procedural acts provided in the Code of Criminal Proceedings (the Code) independently unless the permission of a court or the permission or order of a Prosecutor's Office is required according to the law.[111]

The investigative bodies may make inquiries on the permission of the Prosecutor's Office to electronic communications undertakings about the data required for the identification of an end-user related to the identification tokens used in the public electronic communications network[112] if this is unavoidably necessary for the achievement of the objectives of criminal proceedings. Section 215 of the Code, combined with subsections 90^1(1) and 90^1(3) of the Code, provide the equivalent of Art. 18 of the Cybercrime Convention and grants the Public Prosecutor the power to issue production orders.[113] Search and seizure of stored computer data is covered by section 91 of the Code. Subsections 111^1(2) and 111^1(3) of the Electronic Communications Act together with subsection 90^1(2) of the Code cover the collection of information concerning messages transmitted through commonly used technical communication channels, in other words, the power to order production of traffic data, as provided by Art. 20 of the Cybercrime Convention. Interception of content data, an investigatory power covered by Art. 21 of the Cybercrime Convention, is implemented by subsection 123^3(2)(2) together with section 126^7 of the Code, which regulates wiretapping or covert observation of information transmitted through technical communication channels or other information.

Multistakeholder initiatives

In the area of cyber incident prevention and cooperation, CERT-EE operates the Virtual Situation Room (VSR) which is a collaboration tool for crisis prevention and risk management where service providers, government agencies and service providers themselves can cooperate.[114] The VSR is a single communication platform for sharing situational data between companies providing vital services (such as electricity, data communications, water, fuel supplies, public transport) and government agencies responsible for detecting, managing and preventing crises. The VSR records all crisis management communication and decisions together with situational data which enables the improvement of risk management procedures. In order to be effective, the data that is shared

[111] Ibid, subsections 32(1) and 212(1).

[112] Except for the data relating to the fact of communication of messages, see subsection 90^1(1) of the Code of Criminal Procedure.

[113] Subsection 90^1(1) and 90^1(3) of the Code of Criminal Proceedings. The inquiry may concern the following data: (i) user IDs allocated by the communications undertaking; (ii) user ID of the incoming communication in the mobile network; (iii) the name and address of the customer to whom an IP address, user ID or telephone number was allocated at the time of communication; (iv) user ID and number of the intended recipient of the internet telephony communication; (v) the name, address and user ID of the intended recipient of the e-mail and internet telephony service; (vi) start and end dates and times of the Internet session, IP address allocated by the Internet service provider to the user; (vii) the start (log-in) and the end (log off) date and time of the e-mail or internet telephony service; (viii) the used Internet service of e-mail and Internet telephony services; (ix) the caller's number in case of a dial-up Internet connection; (x) Digital Subscriber Line (DSL) or other end point identifier of the originator of the communication.

[114] See https://www.ria.ee/vsr/.

with the CERT-EE must be up to date. It is highly sensitive information in nature for the service providers; therefore, the confidentiality of this information is of utmost importance.[115]

3.3.3 Germany

Launched in 2011, the German National Cyber Security Strategy[116] aims at protecting Critical Infrastructures, securing IT systems in Germany, strengthening IT security in the public administration, establishing a National Cyber Response Centre and a National Cyber Security Council, effective control of cyber crime and coordination of cyber security in Europe and worldwide, use of reliable and trustworthy IT, development of personnel development in federal authorities, developing tools to respond to cyber attacks. The document mentions the on-going efforts to tackle botnets undertaken by the G8 and the participation of Germany therein, while explicitly addressing the issue of large-scale attacks against critical infrastructure.[117] Recent concepts of multi-stakeholder participation and shared cyber security responsibilities are insufficiently presented in the strategy, seemingly as result of the time in which it was issued. However, recent developments of cyber security initiatives in the country demonstrate the collaborating effort between private and public actors in fighting botnets.

CERTs/CSIRT

Germany uses several Computer Security and Incident Response Teams, distributed in sectors, such as Service Providers, Research and Education, Finance, Commerce, and ICT vendors, as well as among public institutions. Additionally, CERT-Bund,[118] a national governmental institution that is part of the German Federal Office for Information Security (BSI), is responsible for monitoring IT incidents and acting as the main point for prevention and response against cyber incidents. CERT-Bund regularly issues feeds that raise awareness on vulnerabilities and on how to protect computers from attacks, supports efforts to respond to IT security incidents, issues recommendations on cybercrime mitigation, and operates Germany's national IT Situation Centre. The early warning information service (WID) operated by CERT-Bund is distributed among the federal administration, critical-infrastructure companies, citizens and other CERTs. CERT-Bund operates 24-hour on-call duty, alerting public authorities in case of imminent threats, and offers additional tools, such as Bürger-CERT,[119] which informs and warns citizens and small businesses about viruses, worms and other threats.

As described in their RFC2350 document, CERT-Bund does not publish incident-related information (e.g. names, technical details) without the consent of the parties involved. Certain circumstances may require disclosure of these types of information, for instance, to foster closer

[115] Ibid.
[116] See: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile
[117] HAM Luijf, Kim Besseling, Maartje Spoelstra, and Patrick de Graaf, 'Ten National Cyber Security Strategies: A Comparison' in S Bologna et al. (eds.), *Critical Information Infrastructure Security* (Springer 2013).
[118] See https://www.cert-bund.de/
[119] See https://www.buerger-cert.de/

cooperation between affected ISPs or hosting providers, on the basis of CERT-Bund's participation in the FIRST network, and if the attack involves parties of the Bun-CERT constituency. Moreover, information may also be disclosed for supporting the tasks of the law enforcement (albeit there is no regulation in Germany requiring CERT-Bund to do so), the analyses conducted in the National IT Situation Centre, and the Federal Ministry of Interior's situation centre. CERT-Bund reported efforts against botnets include the discovery of a Unix botnet in 2014 via Operation Windingo, which involved private and public sector agents.[120]

Applicable framework

Criminal offences

As discussed, multiple criminal offences can be committed via botnets. The German Criminal Code (Strafgesetzbuch) criminalises as data espionage (Section 202a) with a maximum of 3 years of imprisonment, defined as the unlawful obtaining of data protected against unauthorised access. Data espionage can thus be read as a general hacking offence in German criminal law. However, for the purpose of the German Criminal Code, data espionage is only configured if the perpetrator circumvented a protective mechanism in the process. The preparatory acts towards data espionage are criminalised under Section 202c with penalty of imprisonment not exceeding one year or a fine for whoever produces, acquires for himself or another, sells, supplies, disseminates or makes otherwise accessible passwords or security codes enabling access to data.

Whoever develops bot malware can be liable to imprisonment for up to 5 years in the terms of Section 263a – Computer fraud. Paragraph 1 of Section 263a defines computer fraud as damaging the property of another by influencing the result of data processing through incorrect or unauthorized influence on the course of processing of data, with the aim of obtaining an unlawful profit. Again, preparatory acts configure a criminal offence in itself, for which the perpetrator will be liable with imprisonment for up to three years. Moreover, Section 303b – Computer sabotage is largely applicable to DDoS attacks. In the terms of the provision, whoever causes considerable data processing interference by unlawful data interference, entering or transmitting data with the intention of causing harm, or destroying, damaging, rending unusable, removing or altering a data processing device is liable for the offence. Aggravated forms with imprisonment penalties of up to 10 years are established for interferences causing major financial losses to companies, connected to criminal organisations or compromising critical infrastructures.

Investigatory powers

German law attaches a constitutional value to the activities of law enforcement in limiting these interventions in the rights and liberties of citizens.[121] The current German Criminal Procedure Code (Strafprozessordnung, hereinafter: GCPC) dates from 1887 and although several legislative

[120] See http://www.eset.com/int/about/press/articles/article/operation-windigo-largest-server-botnet-uncovered/

[121] Antje Pedain, 'German criminal procedure' (University of Cambridge, Faculty of Law 2006). Retrieved from http://www.law.cam.ac.uk/faculty-resources/summary/german-criminal-procedure/6368

reforms have followed ever since, the original structure of the code has remained the same since its enactment. Germany ratified the Cybercrime Convention and adapted its body of laws to comply with the provisions of the international instrument. As a consequence, the investigatory powers of German law enforcement can be analysed in light of the convention.

The production order (Art. 18 of the Cybercrime Convention production order) is implemented by Section 95 of the GCPC and Sections 112 and 113 of the German Telecommunications Act. Section 112 of the German Telecommunications Act expressly obliges any publicly available telecommunications services to store customer data files and to provide these data to courts and criminal prosecution authorities, and to federal and state police enforcement authorities for purposes of averting danger.

With respect to computer data, Sections 94, 95, 102, 103, 105 and 110(3) of the GCPC deal with particular aspects of search and seizure in the course of criminal investigations (Art. 19 of the Cybercrime Convention). Section 94 establishes that objects that may be of importance as evidence for the investigation shall be seizer or otherwise secured, regardless of the resistance presented by the person holding the custody of the object. Section 95 continues to determine an obligation to surrender. The order to seizure, as clarified in Section 98, is an exclusive competence of the court, which can be exceptionally granted to public prosecutors and assisting agents. Data search in respect of the suspect is enabled by Section 102 of the GCPC, which allows for the search of the property and of the private and other premises of a suspect, including cases in which the search is believed to lead to further evidence. Section 103 broadens the scope of search and seizure to other persons, admissible for the purpose of apprehending the suspect or to investigate the traces of the offence or to seize other objects, whenever certain facts support the conclusion that the person, trace or object sought is located on the premises to be searched.

Section 105 determines searches may be ordered only by the judge and, in exigent circumstances, also by the public prosecution office and the officials assisting it. The scope of search powers is complemented by Section 110(3), which determines that the examination of an electronic storage medium at the premises of the person affected by the search may be extended to cover physically separate storage media. The use of Section 110(3) is possible insofar as the separate storage media are accessible from the initial storage medium and if there is a concern that the data sought would otherwise be lost. An accurate evaluation on the use of the provisions, especially in regards to jurisdictional limitations, must follow analysis of case law, which goes beyond the scope of this report.

Real-time collection of traffic data (Art. 20 of the Cybercrime Convention) is covered by Section 100g and 100j of the GCPC. The GCPC provides a detailed framework for data production requests to telecommunications providers in relation to a suspect of a crime. Section 100g on Information on Telecommunications Connections establishes that if certain facts give rise to the suspicion that a person, either as perpetrator, inciter or accessory, has committed a criminal offence, to the extent that this is necessary to establish the facts or determine the location of the accused, traffic data may be obtained also without the knowledge of the person concerned. Section 100j on Request for Information can be used to obtain data such as traffic data and IP address for the purpose of clarifying facts or locating the accused.

Finally, interception of content data (Art. 21 of the Cybercrime Convention) is covered by Sections 100a and 100b of the GCPC, which establish the conditions to intercept communications and the official requirements of the interception order. An order to intercept communications may be ordered by the court only upon application by the public prosecution office. In exigent circumstances, the public prosecution office may also issue an order, which shall become ineffective if it is not confirmed by the court within three working days. The order shall be limited to a maximum duration of three months.

Mitigation efforts

German authorities have been prominently active in international efforts against botnets. International consortia involving Dutch law enforcement were responsible for disrupting ZeroAccess,[122] GameOver Zeus & Cryptolocker,[123] Ramnit,[124] and, more recently, Beebone (AAEH),[125] benefiting a large sum of users worldwide. The following paragraph gives a brief overview of the Ramnit takedown.

In February 2015, the German Federal Criminal Police Office (BKA) efforts against the Ramnit botnet infrastructure were successful. The takedown was a coordinated endeavour led by BKA and the Joint European Cybercrime Action Task Force (J-CAT).[126] With an estimated 3.2 million infections, Ramnit is a variety of bank Trojan designed to harvest banking credentials, passwords, cookies, and personal files from victims.[127] Ramnit was also capable of monitoring a victim’s browsing activities, manipulating banks’ websites, scanning a computer’s hard drive and stealing files, among other criminal activities.[128] The consortium acted in different countries and with the support of large companies, including Microsoft, AnubisNetworks and Symantec. The disruptive efforts shut down the command and control servers connected to Ramnit, and worked towards redirecting over 300 domains associated with the fraudulent activities. Press releases issued by authorities involved in the case have called users to verify their systems through special tools made available online.

[122] https://www.europol.europa.eu/content/notorious-botnet-infecting-2-million-computers-disrupted

[123] https://www.europol.europa.eu/content/international-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware

[124] See https://www.europol.europa.eu/content/botnet-taken-down-through-international-law-enforcement-cooperation

[125] See https://www.europol.europa.eu/content/international-police-operation-targets-polymorphic-beebone-botnet

[126] According to Europol, J-CAT was initiated by Europol's EC3, the EU Cybercrime Taskforce, the FBI and the NCA, and the J-CAT comprises a team composed of Cyber Liaison Officers from committed and closely involved Member States, non-EU law enforcement partners and EC3. Retrieved from https://www.europol.europa.eu/content/expert-international-cybercrime-taskforce-launched-tackle-online-crime

[127] http://www.symantec.com/connect/blogs/ramnit-cybercrime-group-hit-major-law-enforcement-operation

[128] Anubisnetworks, ‘Ramnit Takedown Operation’ (White paper, case study 2015). Retrieved from https://www.anubisnetworks.com/white-papers/case-study-ramnit-takedown-operation

Multistakeholder initiatives

The German Anti-Botnet Initiative is an industry initiative for enabling better detection, response and consumer protection. Officially launched in 2010, hosted by ECO (the association of German ISPs) and supported by the Federal Office for Information and Security (BSI), botfrei.de stimulates cooperation and accountability of private sector in combating cybercrime. The adopted strategy works in three levels: 1. Identification of compromised users; 2. User notification; 3. Disinfection support via a national support centre. Identification of victims is made possible by information sharing between private sector partners and further analysis of the data. Data feeds on detected malware are distributed among partners, which are then responsible for alerting compromised customers. The notification is accompanied by information about the national support centre, which offers online disinfection tools in their website and a central help desk. Support via the help desk is provided via ticket numbers distributed by the informing ISPs, protecting the privacy of the infected user, whose identity is preserved in the process. Due to the ticket system, ISPs don't enter personal customer information in the central data base.[129] Exceptionally, this information could be entered for allocation reasons; however, only the project management and the second level senior help desk agents would be granted access to it. The approach implemented in Botfrei has been developed in consultation with the German Federal Data Protection Commissioner. In 2013, ECO and partners started the ACDC project,[130] an EU-funded initiative with the purpose of expanding botfrei.de to other Member States.

3.3.4 The Netherlands

The 2013 Dutch *National Cyber Security Strategy 2 – from awareness to capability* (NCSS 2) recognises botnets as a threat to national cyber security. As described in the report, citizens, businesses and governments are highly targeted by botnets, becoming victims of cybercriminals. It follows that the NCSS 2, especially regarding botnets, is a miscellany of initiatives and actions by the public and private sectors. Efforts to regulate botnets follow the formal legislative procedure, aligned with the civil law tradition of the country. In this regard, the NCSS 2 expressly states the need for more effective and efficient enforcement of cybercrime legislation, with clear norms. To that end, the Netherlands aims to strengthen its legislation by updating the applicable laws, including the Dutch Criminal Code and Criminal Procedure Code. The NCSS 2 would have been a good opportunity for the policy makers to provide further clarity on how to strengthen law enforcement tasks.

Currently, the long-awaited Computercriminaliteit III (Computer Crime III) Bill (hereinafter CC III) has, as of September 2015, still not been introduced in parliament. Moreover, it is already clear that CC III by itself will not attain all the objectives set forth in the NCCS 2. The hard law approach, of which CC III is an example, is supplemented by other, voluntary, arrangements in the form of public-private partnerships and cooperative networks that bring together different

[129] See http://www.oecd.org/sti/ieconomy/45509383.pdf

[130] See https://www.acdc-project.eu

stakeholders working to reduce botnet infections. These partnerships and networks work either on a permanent basis, for instance, sharing best practices and infection data, or ad hoc, addressing particular investigations. The shared responsibilities system for cybersecurity, as defended in the NCSS 2, asserts the existence of duties for both the private and the public sector to act in ensuring cleaner information systems.

CERTs/CSIRT

The National Cyber Security Centre (NCSC) performs the activities of the national computer emergency response team in the Netherlands. Additionally, several non-governmental CERTs coexist,[131] many of them affiliated to the FIRST network.[132] The mission of NCSC is to contribute to improved resilience of networks in the Netherlands, acting as the main point of contact in the country for cybersecurity incidents. The responsibilities of the NCSC include the operational coordination of IT crises and the Dutch central government CERT, response to threats and incidents, perception and action prospects, and fostering cyber security collaboration.

Officially, the NCSC is a division of the Cyber Security Department (DCS), part of the National Coordinator for Security and Counterterrorism (NCTV), within the Ministry of Security and Justice. Despite its governmental constituency, the NCSC works in collaboration with private sector. The NCSC makes use of two tools to monitor the threats and vulnerabilities of Dutch networks, namely Taranis and Beita. Taranis works as an application for data collection and analysis, enabling experts to send warning to interested parties. Beita is a set of spread honeypots installed in governmental organisations, acting as a tool for automatic monitoring of attacks. By collecting attack data, Beita offers a deeper insight into the operation of the malware, which contributes to developing better response. Within the structure of the NCSC, a National Response Network (NRN) was created in 2014, approximating the activities of the NCSC and public-private IT response actors in different sectors with the purpose of sharing scarce resources. NRN is expected to expand in 2015. A counter part of the NRN, the National Detection Network (NDN) works on a similar basis, enabling timely sharing of resources that may help parties take appropriate measures to prevent or minimise damages. NCSC has been involved in the activities that disrupted Pobelka and Bredolab (back then as GOVCERT.NL), as well as in more recent international consortia.

Applicable framework

The Dutch Criminal Code and the Dutch Criminal Procedural Code are the main sources of legal provisions directly applicable to botnets and their investigation. Because a botnet develops in phases, as discussed before, it is possible to identify multiple criminal offences that may apply to the same botnet attack. Therefore, defining which legal provisions are applicable depends on the architecture of the botnet and the concrete circumstances of how it is created and used. Moreover,

[131] See http://www.cert.nl/english
[132] See https://www.first.org/members/map#NL

criminal conducts performed by botnets can be classified under various separate criminal offences. Thus, determining how a real life attack fits the categories of the law requires a detailed examination by the judicial authorities. The following sections provide an overview of the substantive criminal provisions that could be used to criminalise botnet activity and related offences, focusing on criminal attacks against information systems, and of the main criminal investigation powers relevant for investigating botnets.

Criminal Offences

Bot-masters may incur several criminal offences when developing and deploying a botnet, including traditional crimes of fraud and forgery. For the purpose of this report, the analysis is restricted to cybercrime provisions in the narrow sense, i.e., offences against the confidentiality, integrity or availability of computers, computer networks, or computer data.

Bot exploitation is a hacking offence under Dutch criminal law, described as the intentional and unlawful intrusion into a computerized device or a part thereof.[133] Hacking is punished with imprisonment of up to two years for the basic offence of unlawful access, and up to four years in its qualified forms (copying data or hacking onwards from the hacked computer), as stipulated by Art. 138ab of the Dutch Criminal Code (Wetboek van Strafrecht, hereinafter DCC).[134] Moreover, creating a bot also amounts to data interference as defined in Art. 350a, para. 1 of the Dutch Criminal Code,[135] as infecting a computer with malware is an intentional and unlawful form of

[133] See Hoge Raad [Dutch Supreme Court] 22 February 2011, ECLI:NL:PHR:2011:BN9287, which qualifies infection with a virus is a form of hacking.

[134] Evert F Stamhuis, 'Criminal Law on Cyber Crime in The Netherlands' (Preparatory Colloquium, 28-30 November 2012, Verona (Italy), Section I - Information Society and Penal Law). Available at http://www.penal.org/sites/default/files/files/RV-11.pdf
Art. 138ab DCC
(1) A person who intentionally and unlawfully intrudes into an automated device or part thereof is guilty of computer intrusion and liable to a term of imprisonment of not more than one year or a fine of the fourth category. Intrusion includes access:
a. by breaching a security device,
b. by a technical operation,
c. with the help of false signals or a false key, or
d. by assuming a false capacity.
(2) Computer intrusion is punishable by a term of imprisonment of not more than four years or a fine of the fourth category, where the offender subsequently, for his own use or for that of another, copies, taps or records the data stored, processed or transferred in the automated device in which he has intruded.
(3) Computer intrusion committed through a public telecommunication facility is punishable by a term of imprisonment of not more than four years or a fine of the fourth category, where the offender subsequently
a. uses processing capacity of an automated device with the purpose of obtaining unlawful benefit for himself or for another person;
b. through the automated device into which he has intruded gains access to the automated device of a third person.

[135] Stamhuis 2012.
Art. 350a DCC
(1) A person who intentionally and unlawfully alters, erases, renders useless or inaccessible data stored, processed or transferred by means of an automated device or by telecommunication, or adds other data thereto, is liable to a term of imprisonment of not more than two years or a fine of the fourth category.
(2) A person who commits the offence specified in section 1 after having unlawfully intruded, through a public telecommunication facility, into an automated device, and there causes serious damage with respect to such data, is liable to a term of imprisonment of not more than four years or a fine of the fourth category.
(3) A person who intentionally and unlawfully provides or disseminates data designated to cause damage in an automated device, is liable to a term of imprisonment of not more than four years or a fine of the fifth category.
(4) A person who commits the act specified in section 3 with the object of limiting the damage resulting from such data is not criminally liable.

altering data in, or adding data to, a computer. It can also be qualified under Art. 350, para. 3 DCC as a form of making available or disseminating data intended to inflict damage in a computer system, an offence that is punishable with imprisonment for maximum four years. Art. 350a, para 3 DCC applies to distribution of malware such as worms, trojans and viruses.[136]

In the context of botnets, dissemination and exploitation of a bot are the first stages of the overall development of the malicious network, corroborating the idea of hacking as a gateway to other crimes.[137] If not disrupted before completion of the recruitment phase, the botnet will progress to execute the planned attack or become available for sale. In both cases, the idea is to generate a gain to the botmaster. If the botnet is deployed to commit a DDoS attack, the offender will commit the offence of Art. 138b of the Dutch Criminal Code,[138] which penalises with imprisonment not exceeding two years whoever intentionally and unlawfully obstructs access to or use of an automated work by offering or sending data to it. For DDoS attacks on computers with a public function (e.g. government websites), the provision on computer sabotage of Art. 161sexies DCC applies, punishable with a maximum of six years' imprisonment if provisioning of services is disturbed. This provision has even been applied to the infection of a substantial number of end-user computers with malware (the Toxbot virus), as the Supreme Court argued that this also threatened the delivery of services by making it impossible for end-users to safely use Internet banking services.[139] This interpretation has been criticised in the literature, as it seems more appropriate to restrict the application of the provision on computer sabotage to attacks on service providers' computers, not attacks on end-user computers.[140] Finally, if the bot includes a keylogger function (recording and secretly sending keystrokes to the botnet operator), this qualifies as a form of illegal interception (Art. 139c DCC).

Investigatory powers

The task of the Dutch police, as clarified in the Police Act, is to enforce the legal order, and assist those who need help (Art. 3 Police Act 2012). After being notified of a criminal offence, the police start a pre-trial investigation, with the purpose of gathering information about the offence and the suspect.[141] For investigating botnets, they can use all the main powers included in the Cybercrime

[136] Bert-Jaap Koops, 'Cybercrime Legislation in the Netherlands' (2010) 14.3 Electronic Journal of Comparative Law.

[137] Rutger Leukfeldt, Sander Veenstra, and Wouter Stol, 'High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands' (2013) 7 International Journal of Cyber Criminology 1, p. 2. Retrieved from http://www.cybercrimejournal.com/Leukfeldtetal2013janijcc.pdf

[138] Stamhuis 2012.
Art. 138b DCC - A person who intentionally and unlawfully obstructs the access to or the use of an automated device by offering or sending data to that device is liable to a term of imprisonment of not more than one year or a fine of the fourth category.

[139] Hoge Raad [Dutch Supreme Court] 22 February 2011, ECLI:NL:PHR:2011:BN9287.

[140] Jan-Jaap Oerlemans and Bert-Jaap Koops, 'De Hoge Raad bewijst een slechte dienst in high-tech-crimezaak over botnets' (2011) 86 Nederlands Juristenblad 1181.

[141] Peter JP Tak, 'The Dutch criminal justice system: organisation and operation' (Wetenschappelijk Onderzoek- en Documentatiecentrum 2003), p. 25. Retrieved from https://www.wodc.nl/onderzoeksdatabase/w00205-the-dutch-criminal-justice-system-organization-and-operation.aspx

Convention.[142] These investigation powers can be used—although subject to certain conditions, depending on the particular power—for investigating all cybercrimes, including botnet infection and botnet exploitation.

The production order (Art. 18 Cybercrime Convention) is implemented in two sets of powers, one for subscriber data of users of communications services (art. 126n, 126na Dutch Criminal Procedure Code (Wetboek van Strafvordering)) and one for other types of data (art. 126nc et seq. DCPC). Particularly relevant for botnet investigations is the power to order production of identifying data (Art. 126na DCPC), granting police the right to request the provider of a communications service to deliver identifying data such as name, address, postal code, birth date, etc., concerning a user of that service. This power can be used without authorisation from the Public Prosecutor or investigative judge.

Search and seizure of stored computer data (Art. 19 Cybercrime Convention) is implemented in the regular provisions on search and seizure (Articles 95 et seq. DCPC) and in specific powers to search and copy computer data (Articles 125i et seq. DCPC). This includes the power to conduct network search, enabling the police to search computers connected to devices on the place of the search, insofar as the people living/working in the searched location have lawful access to those systems.[143] For data protected by security mechanisms, Art. 125k offers police the power to order to someone other than the suspect the undoing of a security measure (Article 125k, para. 1), and to order the decryption of data (Article 125k, para. 2 DCCP). Search and seizure is, however, less suitable for investigating botnets, at least not in the earlier stages of the investigation, as the location of (computers of) the suspect—and thus the place to be searched—will usually not be known.

For real-time collection of traffic data (Art. 20 Cybercrime Convention), the police can order production of traffic data (art. 126n DCPC), which allows determining the paths of botnet traffic, potentially indicating the source of an infection or commands from the botnet operator. This power requires authorisation from the Public Prosecutor (and in the future, possibly from the investigative judge, in light of the developments in the regulation of data retention[144]). Art. 126m DCPC regulates interception of content data (Art. 21 Cybercrime Convention), covering the interception of both public and non-public communications services. Interception is only allowed when the offence at issue has seriously breached the legal order ('ernstige inbreuk op de rechtsorde'), and it requires a court order.

Overall, the investigatory powers can be used to resolve concrete offences, but they are also usable for the purpose of proactive investigation of organized crime (i.e., without evidence that a specific crime has been committed; it suffices that there are grounds to believe that crimes are

[142] For an overview of investigatory powers applicable to cybercrime investigations, see Tijs Kooijmans and Paul Mevis, 'ICT in the Context of Criminal Procedure: The Netherlands' (Preparatory Colloquium, 24-27 September 2013, Antalya (Turkey), Section III: Information Society and Penal Law); Koops 2010.

[143] Kooijmans and Mevis 2013, p. 9.

[144] Cf. Rechtbank [District Court] Den Haag 11 March 2015, ECLI:NL:RBDHA:2015:2498, at §3.11.

being planned in an organized context),[145] which can be relevant for the purpose of fighting criminal organisations exploiting botnets.

Computercriminaliteit III

The currently-available version of the CC III Bill, as released by the government in May 2013 for public consultation, aims to update investigation powers in light of current challenges of fighting cybercrime. Therefore, the CC III targets what they consider to be hampering issues for law enforcement. The memorandum recognises three obstacles to cybercrime investigation, namely, encryption of data, use of wireless networks and cloud computing. Two specific sets of proposed investigation powers are important in discussing botnet mitigation, namely the power to hack into computers (particularly through, but not limited to, infecting a target computer with a Trojan that enables remote control over various computer functions of the hacked computer) and the power for notice and takedown that can be used to disable access to data. Hacking powers (proposed Art. 125ja DCPC) would give police a legitimate ground to investigate suspicious networks or servers, collect information about the botnet, and, for instance, alter the operation of the malicious infrastructure. The power to disable access to data (proposed Art. 125p) deserves particular attention; in the context of botnet mitigation, this power might be used to order providers of communications services (such as access providers) to take down a command-and-control (C&C) server, or, perhaps, to block network traffic coming from infected computers. The power could thus help control contamination of new devices, and possibly takedown botnet C&C servers.

A noteworthy controversy associated with CC III is the possibility, suggested in the draft Explanatory Memorandum, of extraterritorial application of hacking powers by the police. Via CC III, Dutch police would have the prerogative of making use of hacking powers beyond Dutch territory, if the location of the hacked computer is unknown. Here the understanding of prescriptive jurisdiction appears to have been expanded to legitimise cross-border investigations insofar as Dutch criminal law is applicable to the offense. The memorandum argues that for the detection of serious cross-border cybercrimes, the use of investigative powers is essential, even when that means gaining access to networks located outside Dutch territory. It is not clear to what extent CC III would effectively allow Dutch police to conduct cross-border network investigations, even in the absence of international cooperation agreements with foreign states, but the draft memorandum claims the new provisions are in consonance with ‘the current limits of Dutch law and international law’. The argument could benefit from further clarifying how CC III will achieve harmony with international law.[146] Possibly, the explanation and interpretation will be adapted in the version of the Bill that is to be submitted to Parliament.

[145] See Art. 126o et seq. DCPC, and Kooijmans and Mevis 2013, p. 8.

[146] Koops, B.J. & M.E.A. Goodwin (2014), *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*, The Hague/Tilburg: WODC/TILT, §5.2.1, Retrieved from http://www.wodc.nl/onderzoeksdatabase/2326-de-gevolgen-van-cloudcomputing-voor-de-opsporing-en-vervolging.aspx.

Mitigation efforts

Dutch authorities have been prominently active in international efforts against botnets. International consortia involving Dutch law enforcement were responsible for disrupting ZeroAccess,[147] GameOver Zeus & Cryptolocker,[148] Ramnit,[149] and, recently, Beebone (AAEH),[150] benefiting a large number of users worldwide. There have also been national efforts involving Dutch stakeholders; out of these national efforts, two particular botnet disruptions have been selected based on the availability of materials related to the investigations: Pobelka and Bredolab.

A type of Citadel Trojan active since 2012, Pobelka emerged on the radar of the National Coordinator for Security and Counterterrorism (NCTV) and its partners, including the Public Prosecutor and the Police. In September 2012, SurfRight discovered the control server of the attackers behind Pobelka. After expert analysis of Digital Investigations on the modus operandi of the botnet, and in cooperation with Dutch police, a takedown notice dismantled Pobelka operations in the country. The data found in the server revealed that the same organisation behind Pobelka was also responsible for other important cybercrime attacks victimising the country, such as the Dorifel virus.[151] After investigation and analysis of the collected data, the findings of NCTV concluded that the botnet especially targeted Dutch and German users, aimed at manipulating Internet banking data. A critical aspect of Pobelka, explained by the Minister of Security and Justice[152] included the infection computers located in a wide variety of entities, which included business, critical infrastructures and government itself. The Pobelka case was particularly relevant for victimising specific nations, but also for showing how botnets targeting financial transactions can steal a great deal of other sensitive information. In the case of Pobelka, theft of sensitive data affected business and government, posing an alarming threat to society.[153]

First seen in mid-2009,[154] the Bredolab botnet worked as a breed of pay-per-install malware: infected bots were sold and made available for purchasers to install their chosen malware.[155] A fast-growing botnet, Bredolab allegedly reached 30 million victims by October 2010. In 2010, the hosting provider LeaseWeb was made aware of Bredolab infections in their networks, and notified the Dutch National High Tech Crime Unit (NHTCU) of the Dutch police.[156] The police analysis started from the net-flow data shared by LeaseWeb and was later extended by the use of

[147] https://www.europol.europa.eu/content/notorious-botnet-infecting-2-million-computers-disrupted

[148] https://www.europol.europa.eu/content/international-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware

[149] https://www.europol.europa.eu/content/botnet-taken-down-through-international-law-enforcement-cooperation

[150] https://www.europol.europa.eu/content/international-police-operation-targets-polymorphic-beebone-botnet

[151] http://www.surfright.nl/nl/hitmanpro/pobelka

[152] Brief Tweede Kamer Onderzoek Pobelka. Retrieved from https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/nieuwsberichten/analyse-dataset-pobelka-botnet-afgerond/1/BriefTweede%2BKamer%2BOnderzoek%2BPobelka.pdf

[153] Cybersecurity Assessment Netherlands 2013, p. 8.

[154] David Dittrich, 'So you want to take over a botnet...' (Applied Physics Laboratory, University of Washington). Retrieved from https://www.usenix.org/system/files/conference/leet12/leet12-final23.pdf

[155] Brian Prince, 'Bredolab Down but Far from Out After Botnet Takedown' (eWeek 28 October 2010). Retrieved from http://www.eweek.com/c/a/Security/Bredolab-Down-But-Far-From-Out-After-Botnet-Takedown-160657/

[156] D de Graaf, AF Shosha and P Gladyshev, 'Bredolab: shopping in the cybercrime underworld' (International Conference on Digital Forensics and Cyber Crime 2012), p. 5.

wiretaps on 11 LeaseWeb servers to monitor the communication between servers and bots.[157] On October 25, 2010, the NHTCU infiltrated the botnet, taking control over the backend panel of one of the command and control (C&C) servers and discontinued all malicious activity.[158] Bredolab's disruption was in fact the object of the Tolling Project, which involved a consortium of several partners, namely NHTCU, LeaseWeb, the Public Prosecutor, GOVCERT.NL, Fox-IT (a major ICT security company), and the National Forensics Institute (NFI). The project had three actions points on Bredolab: 1. Arresting the offenders; 2. Stopping the communications between bots and C&Cs and 3. Warning infected victims of their contamination. Overall, the three objectives were attained. Nevertheless, the developments associated with the three action lines raised important legal considerations around jurisdictional competence of the Netherlands, interference with computer data and communications by the police, and hacking powers of law enforcement.

To complete action line 3, the NHTCU developed a warning program to inform victims of the infection in the form of a pop-up message appearing on infected computers' screens. After several days, the NHTCU terminated all communications between affected bots and the server.[159] The NHTCU and the Public Prosecutor justified the intrusion based on public interest and security. However, police use of the botnet infrastructure to push notifications and interrupt communications raised questions over the legality of these actions. The question was raised whether law enforcement was authorised to access end-user computers by using the illegal (as being part of the botnet) connection between the C&C server and infected computers and, if they were, to what extent these powers were balanced against fundamental rights. As noted by Koning,[160] by using decryption keys to penetrate the servers and secretly monitoring communications for about ten weeks, the NHTCU had at its disposal a large and valuable set of data, amounting to serious interference in the privacy of the suspect. The overall situation also infringed the fundamental rights to privacy and data protection of the victims, who were located in many different jurisdictions beyond the Netherlands. These events gave rise to heated legal discussions, reflected in the proposed Computercriminaliteit III Bill (see above).

Multistakeholder initiatives

One additional element of the NCSS 2 is worth noting: the focus on partnerships. The strategy of the Dutch government demonstrates important changes in the approach adopted since the first edition of the document, in 2011. According to the Dutch NCSS 2, the model currently pursued in the country fosters public-private participation networks for improving cybersecurity, instead of the traditional public-private partnership model. Additionally, it presents further clarity on the roles and responsibilities cyber security, and the political will to make the Netherlands a vanguard nation in strengthening investigation and prosecution of crimes, updating the current legal framework.

[157] Ibid.

[158] Ibid, p. 6.

[159] De Graaf, Shosha, and Gladyshev 2012, p. 6.

[160] ME Koning, 'Terug-hacken als opsporingsmethode' (Universiteit van Amsterdam 2011). Retrieved from https://merelkoning.nl/wp-content/uploads/2012/06/Terughacken-als-opsporingsmethode-scriptie-Merel-Koning-september-2011-nn.pdf, p. 18.

There is a clear interest of the Netherlands to strengthen and expand international partnerships at the State level, for instance at the Council of Europe and at Europol (EC3). Another example is ISAC®, which refers to the Information Sharing and Analysis Centers.[161] Following the example set by the United States, ISAC is an initiative to develop a knowledge network on integral safety, security, critical infrastructure, safe cities, organizational security and social security. ISAC also works at the European level and one example of ISAC Europe's collaborative work is in the area of 'resilience engineering, which tries to enhance the ability of organizations to create processes that are robust yet flexible, to monitor and revise risk models, and to use resources proactively in the face of disruptions or ongoing production and economic pressures. To accomplish this task, ISAC Europe works together with The Hague Centre for Resilience and Societal Security, the Centre for Security, Safety and Justice, and Delft University of Technology.[162]

Together with a high-level approach, the Netherlands is fostering private-public participation. It is not clear what exactly the NCSS 2 means by the term, since the strategy provides no further guidance on the matter. It seems to indicate that, instead of public-private partnerships, the idea is for the private sector to play a leading role in cybersecurity beyond individualized activities. It will be interesting to see if there is in fact a change in policy and perspective on the hierarchy between private and public sector in this regard, or if the distinction is merely semantics. In any case, multiple anti-botnet initiatives are currently active in The Netherlands; this section provides a brief overview of the best-known initiatives.

AbuseHUB

AbuseHUB is an initiative of the Abuse Information Exchange platform, a partnership between Dutch ISPs and non-ISPs for improving cybersecurity.[163] AbuseHUB works as a clearinghouse for collecting, analysing and correlating large amounts of abuse data linked to infected devices. The network is a joint effort of nine ISPs, the .nl registrar (SIDN) and the national research and education network operator (SURFnet). The purpose of the initiative is to improve the levels of botnet mitigation in the group, by sharing critical information on attacks and infections. After the centralized analysis of infection data, information is redistributed to members, who are then notified of infections affecting their users and customers. AbuseHUB members can, in turn, notify end-users about infections involving their network and the spotted machine.

A recent report on the results of AbuseHUB in the country showed that, over time, the proportion of the infected population in AbuseHUB members is decreasing.[164] The study, conducted by Delft University of Technology, looked at global and national data sets, from January 2011 to December 2014. Among other findings, it concluded that infections in AbuseHUB member networks are diminishing faster than in non-members, which are mainly composed of smaller

[161] ISAC® homepage: http://www.isac.farmhouse.nl.
[162] http://www.isac.eu.
[163] See https://www.abuseinformationexchange.nl/
[164] Michel van Eeten et al. 'Evaluating the Impact of AbuseHUB on Botnet Mitigation' (Interim Report 1.0, Delft University of Technology 24 March 2015).

broadband providers and hosting providers, and that these organizations can benefit from joining AbuseHUB to improve botnet mitigation.

PPS botnet

The PPS botnet is an initiative of the Dutch Ministry of Economic Affairs to stimulate self-regulation and cooperation in the field of botnets. Thus, a working group was created as part of the public-private program Digiveilig. Based on research conducted by Delft University of Technology, which exposed that most ISPs did not have complete understanding of the amount of infections affecting their networks, the working group started as cooperation between private partners. As a result, the working group brought together ISPs to work together towards sharing and using information on botnet infections and other internet abuse by centrally collecting, analysing and correlating information from various national and international sources. This initial effort led to the creation of the current Abuse Information Exchange.

After Abuse Information Exchange became operational, the working group continued to try to broaden the scope of anti-botnet activities and to extend the cooperation between Economic Affairs and the private sector (Abuse Information Exchange) to the whole chain of partners active in this field. The working group decided to join forces with a parallel botnet working group under the chair of the Ministry of Security and Justice, which involved the police, law enforcement, telecom authorities, the National Cyber Security Centre and the Ministry of Security and Justice and the Ministry of Economic Affairs.

BotLeg project

The BotLeg project (2014-2018) is a common effort led by Tilburg University, Abuse Information Exchange, NHTCU, SIDN, SURFnet and LeaseWeb, and funded by the Dutch Organisation for Scientific Research NWO. In this project, Tilburg University and partners investigate the legal issues surrounding public-private partnerships against botnets in The Netherlands and abroad. Anti-botnet PPPs are expanding and multiplying, but fundamental legal questions are left open, and operations seem to operate in a grey zone. Moreover, the traditional powers and procedures used to investigate crime are often inadequate to the cybercrime reality, according to the project group. The BotLeg project investigates the legal limits and possibilities for public-private anti-botnet operations, aiming to raise awareness among stakeholders and enhance legal certainty on the legitimacy of botnet countermeasures. It focuses on two key sectors (telecommunications/Internet and higher education), for which it will develop guidelines and sectoral codes of conduct. The project aims to contribute to clarifying and establishing the boundaries of anti-botnet operations, with the main goal of stimulating lawful and legitimate botnet fighting. It will work to establish what the law should allow for, in light of the current social demands and in order to balance legislation against cybercrime reality. The findings of BotLeg are expected to contribute to a wider dissemination of best practices in combating botnets in The Netherlands and abroad.

Nationale anti-DDoS Wasstraat (NaWas)

The Nationale Anti-DDoS Wasstraat (NaWas) is a private initiative that offers on-demand services against DDoS attacks, with a focus on medium-sized companies and small Internet operators, such as VoIP providers, for whom the operation costs of security mechanisms against DDoS attacks are too costly or out of reach. NaWas operates as centrally located anti-DDoS facilities, verifying and filtering malicious traffic, and forwarding clean traffic back to the Internet company or operator part to the initiative by working together with NL-IX and AMS-IX. NaWas offers small and medium size business the opportunity of protecting themselves against DDoS attacks in a fast and timely manner, without incurring in the costs that larger security infrastructure and technology would normally require.

Trusted Networks Initiative (TNI)

The Trusted Networks Initiative (TNI) is a multistakeholder partnership led by The Hague Security Delta and involves critical-website operators and relevant stakeholders, including ING, Rabobak, SURFnet, SIDN, E-Zorg, Logius, Ordina, among others. The purpose of the initiative is to build a global trust concept on how to website-operators may react to large-scale or persistent distributed denial of service (DDoS) that are resilient to traditional techniques against DDoS attacks. The initiative offers partners tools for risk mitigation control and timely response against DDoS threats via Trusted Routing service, which is facilitated by a dedicated and secure VLAN that enables continue exchanging of mutual traffic between Trusted Networks.

3.3.5 United Kingdom

In 2010, the UK National Security Council considered 'hostile attacks upon the UK cyber space by other states and large scale cybercrime' as one of the highest national security risks, in light of their likelihood and potential impact.[165] Yet, the National Cybercrime Strategy of the UK, launched in the same year, does not provide clear guidelines on the country's policy against botnets, only mentioning the issue in its glossary.[166] The document describes the country's plan for fighting cybercrime, which includes using traditional methods for increasing awareness, improving international cooperation, strengthening legislation and technical capabilities, and cooperating with the private sector. As a follow-up to the UK National Cyber Security Strategy, important agencies were created to strengthen the institutional fight against cybercrime. Among the most relevant results of the strategy is the creation of the UK National Cyber Crime Unit (NCCU), within the National Crime Agency (NCA). Although not making clear reference to botnets, the NCA lists cybercrime among the higher threats to British society, highlighting the risk of DDoS attacks against businesses.[167]

[165] David Cameron, Great Britain and Cabinet Office, 'A Strong Britain in an Age of Uncertainty: the National Security Strategy' (2010).
Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

[166] UK Home Department, Cyber Crime Strategy.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf

[167] See http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime

CERTs

The UK National Computer Emergency Response Team (CERT-UK), launched in 2014, is part of the action included under the UK National Cyber Security Strategy. The mandate of CERT-UK, as defined in the cyber security strategy, includes four main responsibilities, namely acting as the national cyber-security incident management institution, supporting national critical infrastructure business, promoting awareness among different sectors of society, business and public sector, and providing a single international contact point for collaboration with other national CERTs. CERT-UK works with partners from industry and government, promoting exercises, information exchange, and connecting to other CERTs to improve national response to cyber threats.

The activities of the NCA and the NCCU against GameOver Zeus and Cryptolocker contributed to the involvement of CERT-UK in the information-sharing campaign that promoted awareness and disinfection of compromised machines in the UK.[168] In its first annual report, CERT-UK stated botnets were by far the highest abuse type of cyber threat, spreading malware among citizens and organisations.[169] In the 2014-2015, CERT-UK reported Zeus and its variations, ZeroAccess and Conficker as the three most widespread malware in the UK – botnets infecting millions of computers.[170]

Applicable framework

Criminal offences

The first version of the UK Computer Misuse Act (CMA)[171] dates from 1990, following a legislative response to *R v Gold & Schifreen* (1988) because the existing legislation was incapable of responding to computer target crimes.[172] There are three offences described in the Computer Misuse Act: unauthorised access to computer material, unauthorised access with intent to commit or facilitate commission of further offences, and unauthorised modification of computer material. In short, Sections 1, 2 and 3 of the Computer Misuse Act, respectively, criminalise: hacking activities, the commission of hacking activities with the purpose of committing further crimes and unauthorised acts that intend to, or are recklessness to, impair the operation of computers, prevent of hinder access to any program or data held in a computer, or impair the operation of any such program or the reliability of any such data.[173] The sections provide a detailed description of the various actions that fall within the scope of the act. For instance, in the case R v. Lennon (2006) the court expressed its view that Section 3 of the Computer Criminal Act was applicable to DDoS attacks. For the purpose of this report it suffices to say that Sections 1 to 3 of the CMA are sufficient to cover both hacking offences performed by botnets as well as any attacks that impair access to data.

[168] CERT-UK, Quarterly Report, April - June 2014, available at https://www.cert.gov.uk/wp-content/uploads/2014/08/CERT-UK-Quarterly-Report-01.pdf
[169] See https://www.cert.gov.uk/wp-content/uploads/2015/05/Annual-Report-including-4th-Quarter-FINAL.pdf
[170] See https://www.cert.gov.uk/wp-content/uploads/2015/05/Annual-Report-including-4th-Quarter-FINAL.pdf
[171] Available at http://www.legislation.gov.uk/ukpga/1990/18/contents
[172] Flora Teichner, 'Regulating Cyberspace' (15th BILETA Conference, 14 April 2000). Retrieved from http://www.bileta.ac.uk/content/files/conference%20papers/2000/Regulating%20Cyberspace.pdf
[173] Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press 2012), p. 114-115.

Investigatory Powers

The investigatory powers provided under the Computer Misuse Act differentiate between England and Wales, Scotland, and Northern Ireland, making it difficult to draft an overview of the possible investigatory powers granted to law enforcement authorities. Discipline of investigatory powers in relation to crimes regulated under the Computer Misuse Act is covered in the same instrument. Despite being a part to the Cybercrime Convention, the implementation of the instrument into national law was promoted in a less evident manner. As a result, it is not possible to match specific investigatory powers covered by the Cybercrime Convention to provisions enacted by the national legislator.

Art. 18 of the Cybercrime Convention, the production order, is regulated in Schedule 1 of the Police and Criminal Evidence Act 1984. Under certain conditions, a judge can authorise a production order for information stored in electronic form (sections 1-5 of Schedule 1). Art. 19 of the Cybercrime Convention on search and seizure of stored computer data is covered by Sections 10 and 14 of the CMA. Section 10 of the CMA provides that Section 1(1) (hacking activities) have effect without prejudice to the operation of any enactment in relation to powers of inspection (examination in the case of Scotland), search and seizure. Moreover, Section 14(1) specifies that a warrant authorizing a search can be issued by District Judge (magistrates' courts) to enter and search the premises, using reasonable force if necessary, when an offence under section 1 has been or is in the imminence of being committed in any premises, or when evidence shows such an offence has been or is about to be committed. The powers of Section 14(1) do not authorize a search for privileged, excluded and special procedure material, as regulated in Section 9(2) of the Police and Criminal Evidence Act of 1984. The warrant authorizes the seizure of articles that can be reasonably believed to contain evidence that an offence under Section 1 has been or is about to be committed. For the purpose of search warrants, premises are considered land, buildings, movable structures, vehicles, vessels, aircraft and hovercraft.[174] Further guidance on the application to Northern Ireland is provided under Section 16. Art. 20 and 21 of the Cybercrime Convention, which refer to real-time collection of traffic data and interception of content data, are extensively regulated in Part I of the Regulation of Investigatory Powers Act 2000 (RIPA).

Mitigation efforts

The UK has been involved in multiple operations organised in cooperation with Europol. Recently, the UK National Cybercrime Agency (NCA), as informed in their website, has arguably led the efforts that disrupted the Ramnit botnet. The Agency's National Cyber Crime Unit (NCCU) worked with law enforcement from the Netherlands, Italy and Germany, under the coordination of J-CAT (EC3), to takedown the malicious infrastructure. One of the servers connected to Ramnit was reported to be hosted in the county of Hampshire and to infect the computers of 33.000 UK citizens.

[174] Section 14 of the Computer Misuse Act does not extend to Scotland, according to para. (6) of the provision.

After the event, the NCA alerted users about the widespread infection, offering special and free cleaning tools for removing the infection and fixing vulnerabilities.

Multistakeholder initiatives

Launched in 2013, the Cyber-security Information Sharing Partnership (CiSP) counts more than 950 organisations and 2500 individuals who have signed up to receive data.[175] The Cyber-security Information Sharing Partnership (CiSP) is a joint private and public sector initiative in the UK to share information about attacks.[176] The purpose of CiSP is to increase situational awareness and timely information that can help parties improve their prevention and reaction to cyber threats. The information gathered in the platform is further analysed by a team composed of experts from industry and government. After analysis, the information is categorised and distributed to partners via various sources, such as alerts and summaries. The CiSP platform is part of the CERT-UK, benefiting from the information collected by the latter, where they receive customised feeds based on the range of their network, in an allegedly secure and confidential environment. Thanks to its integration within the CERT-UK, CiSP partners were given advanced notice of takedown operations against Gameover Zeus botnet.

3.4 Conclusion

This chapter describes current efforts taken against botnets in the five case study countries. It examines national cybersecurity strategies, CERTs, multi-stakeholder efforts and legislation relevant to countering botnets in national territory and abroad. As far as national cybersecurity strategies are concerned, the documents reflect the high-level goals and principles of each country in the field of cybersecurity. Because national cybersecurity strategies tend to be abstract in nature, no significant reference to botnets could be identified and in many cases it is still necessary to clarify the legitimate grounds for – and limits of – enabling counter-measures against botnets.

Each examined country has in place a national CERT with the mandate to oversee the dissemination of threats on national territory. While the procedures followed by CERTs are to a large extent harmonised, the practical value of their operations in regard to botnets varies largely. In addition, many CERTs distribute relevant information within circles of trust, and since such information is often undisclosed to a larger audience, it is not possible to evaluate the impact and the influence of national CERTs countering botnets beyond of what is made publicly available online. Multi-stakeholder mitigation efforts also seem to vary, while all countries have demonstrated participation in international cooperative efforts against botnets. Initiatives supported by public authorities were easier to identify than sectoral and inter-sectoral efforts. A large part of the international cooperation activities against botnets revealed a connection with EUROPOL (EC3)

[175] CERT-UK, Quarterly Report, April - June 2014, available at https://www.cert.gov.uk/wp-content/uploads/2014/08/CERT-UK-Quarterly-Report-01.pdf

[176] Ibid.

and the FBI efforts in fighting botnets, demonstrating the important role played by both institutions and a significant level of international cooperation.

Legislation was the most harmonised element of this analysis, given that all countries have ratified the Cybercrime Convention. Nevertheless, since the Convention acts as a minimum catalogue of offences and investigation powers, there are differences between countries, with some having wider, broader substantive criminal law, intended to encompass various forms of crime. The legislation of the Netherlands, Estonia and Germany tries to cover a multitude of cybercrime, whereas the U.K. and Canada provide a more flexible scope of criminalisation. This difference could be related to the differences between civil law and common law traditions. In terms of investigatory powers, the same difference becomes clear, as civil law countries show a greater emphasis on the statutory limits of the use of invasive measures. With respect to the legal aspects of botnet mitigation, at the moment ISPs are currently quite limited in the types of action they can take. There are attempts to formalize an increased role for ISPs, but this is currently taking the form of ISPs themselves changing their Terms of Use.

4. Case 2: Protection of Vital Infrastructures

4.1 Introduction

A vital infrastructure can be defined as follows: "A product or service is vital when it either: provides an essential contribution to society in maintaining a defined minimum quality level of (1) national and international law & order, (2) public safety, (3) economy, (4) public health, (5) ecological environment; or when loss or disruption impacts citizens or government administration at a national scale or endangers the minimum quality level."[177]

Recital 4 of the Council Directive 2013/40/EU states, "There are a number of critical infrastructures in the Union, the disruption or destruction of which would have a significant cross-border impact. Critical infrastructures could be understood to be an asset, system or part thereof located in Member States, which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, such as power plants, transport networks or government networks, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions."[178]

The proposed NIS Directive[179] (explanatory memorandum, p.1) refers more specifically to the role of networks: "…critical infrastructures, such as energy, transport, and key providers of information society services (e-commerce platforms, social networks, etc.), as well as public administrations." "The current regulatory framework requires only telecommunication companies to adopt risk management steps and to report serious NIS incidents. However, many other sectors rely on ICT as an enabler and should therefore be concerned about NIS as well. A number of specific infrastructure and service providers are particularly vulnerable, due to their high dependence on correctly functioning network and information systems. These sectors play an essential role in providing key support services for our economy and society, and the security of their systems is of particular importance to the functioning of the Internal Market. These sectors include banking, stock exchanges, energy generation, transmission and distribution, transport (air, rail, maritime), health, Internet services and public administrations."[180]

National vital infrastructures, thus, generally include any combination of the following (with slight variations per country): energy (electricity, gas and oil), telecommunications and ICT (fixed and mobile telephony, radio, broadcasting and Internet), drinking water, food (supply and safety), health (emergency and other hospital care, medicine and vaccines), financial sector (payments and financial transaction government), management of surface water (quality and quantity), public order and safety, public administration (diplomacy, disclosure of information by the government, armed forces and decision making), transport (airports, harbours and waterways, main roads and

[177] EAM Luijf, HH Burger and MHA Klaver, 'Critical Infrastructure Protection in the Netherlands: A Quick Scan' (EICAR conference Best Paper, 2013).

[178] Council Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L218/8.

[179] Proposal for a Council Directive 2013/0027 concerning measures to ensure a high common level of network and information security across the Union [2013] COM (2013) 48 final.

[180] Ibid, p. 4.

railways), chemical and nuclear industry (transportation, storage, production and processing of materials).[181]

This chapter uses a case study of the *energy sector* to examine how vital infrastructures are protected in the selected countries. High profile cases, such as the Dutch Supervisory Control And Data Acquisition (SCADA) incidents,[182] power outages[183] and the Canadian Telvent incident[184] reflect the importance of good cybersecurity in relation to the energy networks. Each country case study provides a stakeholder analysis that briefly outlines:

1) *Who and how* - Which actors are responsible for taking which actions? What is the organisational and institutional arrangement? What is the remit of actors to act?

2) *What and why* - What does the content of the regulation aim to achieve? How are vital infrastructures defined, and which conditions apply for infrastructures to be deemed 'vital'?

3) W*here* - In which places is the challenge being addressed in practice, e.g. sectors, (self)-regulatory arrangements, illustrative cases?

These aspects, taken together, address the following question: *How is continuity of electricity provisioning, particularly the protection against cyber-attacks in the context of the transition towards smart grids, organized?* The cases are discussed in the following order: Canada, Estonia, Germany, the Netherlands and the UK. In each country description, we give an overview of relevant actors and national legislation. Overarching European legislation that applies to Estonia, Germany, the Netherlands and the UK is discussed after the case studies.

4.2 Case Study Countries

Each case begins with a short introduction, followed by an outline of relevant actors and overview of applicable legislation. In examining the regulatory framework for each case, we distinguish between regulation of prevention, regulation of incident management and regulation of repression (although there is occasional overlap). Prevention refers to measures taken to eliminate or limit the consequences of an incident, but typically these measures are taken ex ante, i.e. in absence of any concrete incident. Incident management relates to the measures that are taken in response to a concrete incident in order to eliminate or limit the effects of the incident. Repression comprises the entirety of measures taken to identify and bring to justice perpetrators of attacks. As understood here, this category does not relate to the enforcement of regulation that addresses prevention or

[181] NS van der Meulen and AR Lodder, 'Cybersecurity' in S van der Hof, AR Lodder, and GJ Zwenne, *Recht en Computer* (Kluwer 2014), pp. 301-318.

[182] The SCADA system can be used to control e.g. sluices and swimming pools from a distance via the Internet. It is intended to be used for maintenance, but insufficient security allows seizure of control of the system. In 2012, the Volkskrant reported a security incident in relation to a public swimming pool. See: http://www.volkskrant.nl/recensies/blunder-subtropisch-zwembad-besturingssysteem-stond-wekenlang-open~a3190060/

[183] There was a major power outage in the north of the Netherlands in March, 2015. See, e.g., http://www.nrc.nl/nieuws/2015/03/27/dit-zijn-de-gevolgen-van-de-grote-stroomstoring-in-noord-holland/

[184] Alexandra Posadzki, 'Cyber Security in Canada's Private Sector A 'Significant' Problem: Government Records' *The Canadian Press* (Toronto, 13 September 2013). Available at: http://www.huffingtonpost.ca/2013/07/14/cyber-security-canada_n_3594310.html

incident management (for example enforcement of reporting duties resting on vital infrastructure providers).

4.2.1 Canada

At a general level, cybercrime recently received attention in Canadian policy circles. The Royal Canadian Mounted Police published a document on cyber incidents in Canada. In ‘Cybercrime: an overview of incidents and issues in Canada’, the RCMP reports on cybercrime, focussing on aspects of the cybercrime environment that affect Canada’s public organizations, businesses and citizens in real and harmful ways.[185] It describes Canada’s digital landscape and covers a broad range of cyber incidents. Relevant policy documents include the Cyber Security Strategy of 2010 (NCS 2010),[186] the ‘Action Plan 2010-2015 for Canada’s Cyber Security Strategy’ (APCS 2010),[187] the ‘National Strategy for Critical Infrastructure’ of 2009 (NSCI 2009),[188] and the ‘Action Plan for Critical Infrastructure 2014-2017’ (APCI 2014).[189] The latter two have a broader approach than cybersecurity only. Also relevant is the ‘Policy on Government Security’ of 2009, administered by the Treasury Board Secretariat.

An important aspect of governance in Canada is the division of authority and responsibility between the national/federal government and the provincial governments and territories. With respect to the energy sector, this division is not always clear-cut: “Section 92A of the Constitution Act, 1867 assigned to the provincial governments the exclusive authority to make laws in relation to non-renewable resources and electrical energy, while Section 125 prevented the federal government from taxing any provincial government lands or property. On the other hand, the federal government has the power to make treaties with foreign countries. This has important implications for treaties involving energy production, like the Kyoto Protocol, which the Canadian government signed in 2002. Although the federal government had the authority to sign the treaty, it may require the cooperation of the provincial governments to enforce it.”[190] Any effort to understand governance in general and cybersecurity governance of vital infrastructures in particular must start with understanding this division of responsibilities.

In this section we therefore outline relevant actors in the governance of Canada’s energy sector at both the national and provincial levels, as well as relevant laws – again distinguishing between regulation of prevention, regulation of incident management and regulation of repression.

Relevant Actors

The following actors are relevant to the governance of energy infrastructures:

[185] http://www.rcmp-grc.gc.ca/pubs/cc-report-rapport-cc-eng.htm

[186] Available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/canadaNCSS.pdf

[187] Available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf

[188] Available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf

[189] Available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/pln-crtcl-nfrstrctr-2014-17-eng.pdf

[190] Wikipedia. Available at: http://en.wikipedia.org/wiki/Energy_policy_of_Canada

- Public Safety Canada (PSC) is the federal department/agency for public safety and emergency preparedness. It provides central coordination to address risks within the Government and across Canada.[191] Public Safety Canada also leads public awareness and outreach activities to inform Canadians of the potential risks they face and the actions they can take to protect themselves and their families in cyberspace.[192]
    - Canadian Cyber Incident Response Centre monitors and provides mitigation advice on cyber threats and coordinates the national response to any cybersecurity incident. It falls under the responsibility of Public Safety Canada.
- Foreign Affairs and International Trade Canada advises on the international dimension of cybersecurity and work to develop a cybersecurity foreign policy that will help strengthen coherence in the Government's engagement abroad on cybersecurity.
    - The Department of National Defence and the Canadian Forces works with allies to develop the policy and legal framework for military aspects of cyber security, complementing international outreach efforts of Foreign Affairs and International Trade Canada.
- Treasury Board Secretariat administers the Policy on Government Security, which sets out safeguards to assure the delivery of Government services to Canadians.
- Communications Security Establishment Canada detects and discovers threats, provides foreign intelligence and cyber security services, and responds to cyber threats and attacks against Government networks and information technology systems.
- Canadian Security Intelligence Service analyses and investigates domestic and international threats to the security of Canada.
- The Royal Canadian Mounted Police investigates, as per the Royal Canadian Mounted Police Act, suspected domestic and international criminal acts against Canadian networks and the critical information infrastructure.
- Natural Resources Canada is a sector-specific federal department/agency that is responsible for the national-level sector network 'Energy and utilities', one of the ten vital infrastructures discerned in the NSCI.[193]
- The National Cross Sector Forum is established under the NSCI 2009 to promote collaboration across sector networks, address interdependencies, and promote information sharing across sectors.[194]
- Provinces and territories provide a range of essential services for which delivery is dependent on the safe and secure operation of their cyber systems.[195]

[191] National Cybersecurity Strategy 2010, p.9-10.
[192] The first half of this sketch of actors is taken from NCS 2010, p.10.
[193] Government of Canada, 'Action Plan for Critical Infrastructures (APCI)' (2014), p.3.
[194] Idem.
[195] NCS 2010, p.11.

- Critical infrastructure owners and operators bear the primary responsibility for protecting their assets and services.[196]
- Individual Canadians have a responsibility to be prepared for a disruption of vital infrastructures and to ensure that they and their families are ready to cope for at least the first 72 hours of an emergency.[197]

Regulatory Framework

Regulation of Prevention

The NSCI 2009 identifies three strategic objectives for enhancing the resilience of critical infrastructure in Canada: building partnerships, sharing and protecting information and implementing an all-hazards risk management approach. Public Safety Canada has the task of coordinating implementation of Canada's Cyber Security Strategy and all efforts to secure vital cybersecurity systems. In 2010, the NCS announced that joint public/private sector initiatives to identify and share best practices for addressing threats to the systems of vital infrastructures would be developed.[198] PSC has realised this by formalizing 'partnerships to engage critical infrastructure sectors and government agencies at all levels through the National Cross-Sector Forum as well as the development of a cross-sector agreement for improved information sharing'.[199]

Provincial governments are responsible for oversight of electric reliability standards.[200] Thereto, they have recognized the North American Electric Reliability Corporation (NERC) as the Electricity Reliability Organization responsible for developing mandatory and enforceable reliability standards. 'These reliability standards address issues relevant to the operation of existing, new, and modified bulk-power facilities, including critical infrastructure protection (CIP). CIP standards cover critical cyber asset identification, security management controls, personnel and training, electronic security, physical security, systems security, incident reporting and response planning, and recovery plans. CIP version 5, the most recent set of standards, was approved in 2013.'[201]

Regulation of Incident Management

The Emergency Management Framework for Canada defines a collaborative approach to emergency management and establishes a federal, provincial and territorial partnership for enhancing the public safety of Canadians. The Framework identifies principles of cooperation (i.e. responsibility, comprehensiveness, partnerships, coherency of action, risk-based, all-hazards, resilience, clear communications, and continuous improvement) and it recognizes that emergency

[196] Government of Canada, 'National Strategy for Critical Infrastructure (NSCI)' (2009), p.2. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf.
[197] Idem.
[198] NCS 2010, p.12.
[199] Bipartisan Policy Center, 'Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat - A Report from the Co-chairs of the Bipartisan Policy Center's Electric Grid Cybersecurity Initiative' (2014), p. 30 (hereinafter BPC 2014).
[200] BPC 2014, p. 23.
[201] BPC 2014, p.24-25.

management is comprised of interdependent risk-based functions: prevention, mitigation, preparedness, response and recovery.[202]

"Cyber incident management in Canada is a collaborative and voluntary activity" and "CCIRC cannot compel any organization to take action on its network, and organizations can choose not to report incidents or seek assistance."[203] The Canadian Cyber Incident Response Centre does not have the authority to force companies to comply with its recommendations. According to an academic researcher, the government cannot force companies to report incidents or heed the CCIRC's warnings; Rather, each individual company has the discretion to determine how much to spend on cyber security. "Their assessments about risks and the level of security needed to protect their assets may well differ from what we, as a society, feel is appropriate".[204]

The National Strategy recognizes that the first response in an emergency will almost always be by local owners and operators, the municipality or at the provincial/territorial level. The federal government fulfils national leadership responsibilities relating to emergency management, respecting existing federal, provincial and territorial jurisdiction and legislation. The federal government is also responsible for providing assistance to provinces/territories if the province/territory has requested the assistance.[205]

The documentation accompanying the 2015 Federal budget, published in April 2015, states:[206] “The Government is taking action to protect the vital cyber systems that Canadians rely on daily and that are critical to national security. Following consultations, new legislation will require operators of vital cyber systems to implement cyber security plans, meet robust security outcomes for their systems and report cyber security incidents to the Government of Canada.”[207] The name of the new legislation will be ‘Protection of Canada’s Vital Cyber Systems Act’. More information on the new legislation is not available at the moment of writing. The government is working on the legislation ‘quietly’.

Regulation of Repression

In its 2010 National Cyberscurity Strategy, the Government announced that it would ‘soon introduce legislation to modernize law enforcement’s investigative powers, and ensure that technological innovations are not used to evade lawful interceptions of communications supporting criminal activity’.[208] For more information about this legislation on lawful access, the reader is referred to the corresponding section in the ‘Identity Infrastructure’ case in Chapter 5.

[202] NSCI 2009, p.4.

[203] Josee Picard, a spokeswoman for Public Safety Canada, in: Alexandra Posadzki, ‘Cyber Security In Canada's Private Sector A 'Significant' Problem: Government Records’ *The Canadian Press* (Toronto, 13 September 2013). Available at: http://www.huffingtonpost.ca/2013/07/14/cyber-security-canada_n_3594310.html

[204] Angela Gendron, a senior fellow at Carleton University's Canadian Centre of Intelligence and Security Studies.

[205] NSCI 2009, p.2.

[206] Available at: http://www.budget.gc.ca/2015/docs/plan/ch4-3-eng.html

[207] More information on the new legislation is not available at the moment of writing. Several web-articles state the government is working on the legislation ‘quietly’.

[208] NCS 2010, p. 3

The Royal Canadian Mounted Police will be given the resources required to establish a centralized Integrated Cyber Crime Fusion Centre. This team will increase the ability of the Royal Canadian Mounted Police to respond, using a risk-based analysis approach, to requests from the Canadian Cyber Incident Response Centre regarding cyber-attacks against Government or Canada's critical infrastructure.[209]

4.2.2 Estonia

In Estonia, a vital service is defined as a service that is essential for the maintenance of the society, and the health, safety, security, economic or social well-being of people. The Emergency Act introduces 43 such vital services,[210] with a functioning electricity supply being prominent in that list. As defined in article 2(a) of the Directive 2008/114/EC[211], critical infrastructure (CI) is an asset, system or part thereof, which is essential to the maintenance of vital societal functions, and the health, safety, security, economic or social well-being of people, and whose disruption or destruction would have a significant impact in a Member State as a result of the failure to maintain those functions. The critical information infrastructure (CII) comprises of information and communications systems for which the maintenance, reliability and safety are essential for the proper functioning of a country. As such, the CII is a part of the CI.

The Estonian energy market opened in 1 January 2013. This meant that consumers could choose from different sellers and different price options. The energy provisioning system of Estonia differentiates the suppliers of electricity, electricity distribution network undertakings and sellers. At the moment, there are 12 sellers on the market.[212] According to the Estonian Competition Authority, there are 34 distribution network undertakings.[213] Additionally, Elering AS, a state-owned public limited company, manages the Estonian electricity system.[214] There is one major supplier – Narva Elektrijaamad (90% of the production volume), as well as four cogeneration plants and several smaller alternative energy suppliers.[215]

Estonia has been moving towards smart grid since 2012, when the largest electricity distribution undertaking (Elektrilevi[216]) initiated the move toward smart electricity meters that enable remote meter reading. As a result of a 94 million euro investment,[217] Elektrilevi is to equip every

[209] NCS 2010, p. 13.
[210] See section 34 of the Emergency Act. Also, see <https://www.ria.ee/CIIP/> accessed 29 July 2015.
[211] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. OJ L 345, 23.12.2008, p. 75–82
[212] See http://avatud2013.ee/. Among these 12 sellers, Eesti Energia (formerly the sole seller on the market) holds more than 60 % of the market, the second biggest seller on the electricity market is Elektrum AS. See http://uudised.err.ee/v/majandus/8124f4b1-cb83-4e99-ba82-9561fcafc44b. (Find new ref)
[213] See http://www.konkurentsiamet.ee/file.php?27430. Although the number is large, the largest undertaking is Elektrilevi AS, most of the other 33 undertakings have a very little market share.
[214] See http://elering.ee/en/ and http://elering.ee/the-electricity-system/.
[215] See http://energiasalv.ee/energiasusteem.
[216] According to the website of MEAC, Elektrilevi owns 87.5% of the electricity distribution market. See <https://www.mkm.ee/et/tegevused-eesmargid/energeetika/elektriturg> accessed 29 July 2015.
[217] See <http://uudised.err.ee/v/majandus/863293ec-14f6-4c8b-9bc9-7f1a2785242f> accessed 19 May 2015.

household with a smart meter by the start of 2017. This means replacing approximately 630,000 meters.[218]

Relevant Actors

In addition to the actors mentioned in the introduction, the following actors are relevant to the governance of energy infrastructures in Estonia:

- The Ministry of Economic Affairs and Communications (MEAC) is tasked with protecting the general CI. MEAC is also responsible for the continuous functioning of electricity supply.[219]
- The Information Systems' Authority (ISA) is a sub-department of MEAC responsible for protecting the CII. At ISA, the protection of CII is handled by a specific unit – the Department of Critical Information Infrastructure Protection (the Department).
- The Department of Critical Infrastructure Protection is engaged in the protection of critical information systems at a strategic, rather than operational, level.[220] The Department: i) collects and maintains information on CII; ii) carries out risk assessments on CII; iii) draws up security measures for the protection of CII; and iv) exercises supervision for the proper functioning of CII security measures.[221] Thus, ISA sets the rules how to protect vital services and exercises supervision on the implementation of the measures.

Regulatory Framework

Regulation of Prevention

Emergency Act and Law Enforcement Act

The Emergency Act[222], the main source of law on CI, delineates the obligations of vital service providers (VSPs). According to subsection 37(3) of the Emergency Act, the provider of a vital service is obliged to: i) prepare a risk assessment of the continuous operation of the vital service (risk assessment of continuous operation); ii) prepare a plan for ensuring the continuous operation of the vital service (continuous operation plan); iii) notify ISA of an event significantly disturbing the continuous operation of the vital service or of an impending risk of the occurrence of such an event and iv) upon request, provide information concerning the provision of the vital service to ISA.[223] Subsection 38 of the Emergency Act outlines the necessary components of the risk assessment of continuous operation:

- Risk Assessment of Continuous Operation: The document must include the following: i) the list of risks causing a partial or complete interruption in the provision of a vital service; ii) the probability of a partial or complete interruption in the provision of a vital service; and iii) the

[218] See <http://tarbija24.postimees.ee/3056155/elektrinaidu-teatamisest-saab-kahe-aasta-parast-ajalugu> accessed 23 May 2015.

[219] Section 34(2)(1) of the Emergency Act.

[220] At operational level, the protection of information systems for the provision of vital services is handled by the subunit of ISA – the Computer Emergency Response Team of Estonia (CERT-EE).

[221] See https://www.ria.ee/actions-and-roles/.

[222] The English version of the Emergency Act is accessible here: https://www.riigiteataja.ee/en/eli/524032015001/consolide.

[223] Subsections 37(3)(1) to 37(3)(4) of the Emergency Act.

possible consequences of a partial or complete interruption in the provision of a vital service.[224] The risk analysis is confidential and information contained therein may not be disclosed. The topicality of the risk analysis should be assessed once every two years and necessary amendments should be made.[225]

- Continuous Operation Plan: describes necessary measures for: i) preventing a partial or complete interruption in the provision of a vital service; ii) mitigating the consequences of a partial or complete interruption in the provision of a vital service; and iii) restoring the continuous operation of a vital service in case of a partial or complete interruption in the provision of the vital service. This also constitutes confidential information that may not be disclosed.[226] The need to update the continuous operation plan must be assessed at least once every two years.[227]

In addition to the obligation to draw up the documents described above, the VSPs must immediately notify MEAC (or ISA) of an event that significant disturbs the continuous operation of the vital service or of an impending risk of such and (upon request) provide information concerning the provision of the vital service.[228]

On the basis of the Risk Assessment of Continuous Operation, the VSPs assess whether and to what extent the information systems affect the functioning of the vital service. In the field of electricity supply, the dependence is presumably very large. Therefore, the VSPs[229] are obliged to implement adequate security measures with respect to the information systems used for the provision of the vital service and the related information assets.[230] According to the regulation "Security Measures for Vital Service Information Systems and related Information Assets"[231], the adequate security measures include: limiting access to the critical information systems to authorised personnel only; creating secure authentication procedures for entitled personnel; assuring the creation of an audit trail; drafting reports of security incidents and preserving copies of documents and data that are vital to the provision of the vital service. The latter must be stored in rooms protected against electromagnetic radiation. The regulation urges the VSPs to implement either the ISO/IEC 27001:2006 security standard or ISKE (see below).

Although, the Emergency Act defines the borders and obligations for providers of vital services, the protection of CI and CII can be seen as a cooperative effort between private equity VSPs and the state. Since July 1, 2014, when the Law Enforcement Act entered into force, MEAC and ISA have specific supervisory responsibilities and the right to issue fines to VSPs that do not

[224] Subsection 38(1)(1) to 38(1)(3) of the Emergency Act.
[225] Subsection 38(4) of the Emergency Act. The Minister of Interior has also drafted guidelines for the drafting of the risk analysis – Regulation of the Ministry of Interior of 8 June 2010, number 16. Accessible: https://www.riigiteataja.ee/akt/13326405.
[226] Subsection 39(3) of the Emergency Act.
[227] Ibid, subsection 39(4).
[228] Subsections 37(3)(1) to 37(3)(4) of the Emergency Act.
[229] There are five VSPs in the sphere of electricity provisioning that have to follow these obligations according to the official of the Department of Critical Information Infrastructure Protection.
[230] Subsection 40(1) of the Emergency Act.
[231] Regulation of the Government of the Republic of Estonia number 43 of 14 March 2013. See <https://www.riigiteataja.ee/akt/120032013007> accessed 29 July 2015.

fulfil their obligations under the Emergency Act[232]. According to the interviewed officials of ISA, this change in the Law Enforcement Act has significantly disciplined the VSPs[233]. Although it represents a shift from cooperation-based communication to sanction-based communication between the VSPs and the state, it is a necessary tool due to the dependence of vital services more generally and electricity supply in particular. As of 22 April 2015, no fines had been issued.[234]

ISKE

ISKE was established by Government Regulation in 2008[235] (ISKE Regulation). It is a three-level IT baseline security system analogous to ISO 27000 security standards and is developed and updated by ISA[236]. It is a required security measure for government and state agencies and is a *recommended* standard for VSPs.[237] According to ISKE Regulation, chief processor of a database must conduct an audit, dependent on the security level of the database, every two to four years.[238]

Regulation of Incident Management

On the operational level, CERT-EE is the responsible body managing the cyber incidents. According to the "Emergency Plan in case of a Large Scale Cyber-Attack"[239] (the Plan), a cyber-attack is deemed to be of "large scale" if it is directed against the information systems of the VSP. According to the Plan, the VSP under attack must notify CERT-EE of the occurrence and apply its Continuous Operation Plan to find a resolution and mitigate or restore the functioning of the vital service. The VSP may request the help of Estonian Defence League's Cyber Unit[240] to mitigate the consequences of the large scale cyber-attack.

Regulation of Repression

The Penal Code[241] sets out three provisions criminalising the damaging or hindering of the functioning of the vital services. Subsection 206(2)(3) of the Penal Code stipulates that the illegal alteration, deletion, damaging or blocking of data in computer systems of a vital sector is punishable with up to five years' imprisonment.[242] Subsection 207(2)(3) of the Penal Code stipulates that if the illegal interference with or hindering of the functioning of computer systems by way of uploading,

[232] Section 51 of the Emergency Act. The maximum sanction for failing to draft the Risk Assessment and/or Operation Plan, notify MEAC (or ISA) of a disturbing event or failure to provide documents to MEAC is EUR 6,400.

[233] Interview with U. Sutermäe and M. Vasar (Tallinn, 22 April 2015).

[234] Ibid.

[235] Regulation of the Government of the Republic of Estonia number 252 of 20 December 2007. See <https://www.riigiteataja.ee/akt/13125331?leiaKehtiv> accessed 27 May 2015.

[236] It must be noted that the preparation and development of ISKE is based on a German information security standard – IT Baseline Protection Manual (*IT-Grundschutz*) which has been adapted to suit the Estonian situation. See <https://www.ria.ee/iske-en/> accessed 23 May 2015.

[237] Interview with Urmo Sutermäe (Tallinn, 22 April 2015).

[238] See <https://www.ria.ee/iske-audit/> accessed 24 May 2015.

[239] Regulation of the Government of the Republic of Estonia number 372 of 25 August 2011. See <https://www.ria.ee/public/Kuberturvalisus/ulatusliku_kuberrunnaku_hadaolukorra_lahendamise_plaan.pdf> accessed 3 June 2015.

[240] Estonian Defence League's Cyber Unit <http://www.kaitseliit.ee/en/cyber-unit> accessed 28 May 2015.

[241] See <https://www.riigiteataja.ee/en/eli/519032015003/consolide> accessed 28 May 2015.

[242] Subsection 206(2)(3) of the Penal Code. It must be noted that the Penal Code uses "vital sector" instead of "vital service".

transmitting, deleting, damaging, altering or blocking of data was committed against a computer system of a vital sector or the provision of public services is interfered or hindered thereby, the act is punishable with up to five years' imprisonment.[243] Subsection 406(1) stipulates that knowingly damaging or destroying a structure or device of the energy, communication, signalling, water supply or sewer system, traffic control or other vital public utilities system, if causing danger to human life or health or hindering the proper functioning of a vital public utilities system is an act punishable with up to three years' imprisonment.[244] If the act causes interference with, or interruption of, the functioning of a vital public utilities system, the act is punishable with up to five years' imprisonment.[245,246]

4.2.3 Germany

Ensuring the protection of the German business and industry infrastructure is a central issue of the country's security policy.[247] Infrastructure is considered "critical" whenever it is of major importance to the functioning of modern societies and any failure or degradation would result in sustained disruptions in the overall system (German CIP Strategy 2009). An important criterion for this assessment is criticality as a relative measure of the importance of a given infrastructure in terms of the impact of its disruption or functional failure on the security of supply, i.e. providing society with important goods and services. Such criticality may be of a systemic or symbolic nature or include both elements. An infrastructure will, in particular, be of systemic criticality whenever - due to its structural, functional and technical position within the overall system of infrastructure sectors - it is highly relevant as regards interdependencies; electricity is an example of this (German CIP Strategy 2009). According to the IT Emergency and Crisis Exercises in Critical Infrastructures (2008), the following areas constitute critical infrastructures: Transport and traffic; Energy (electricity, nuclear power plants, mineral oil, gas); Hazardous substances; Information technology and telecommunications; Finance, banking and insurance; Supply systems and Public authorities, government and the judiciary (government institutions). The UP KRITIS Public-Private Partnership for Critical Infrastructure Protection sees the following sectors (see Figure 1) as a part of critical infrastructure:[248]

[243] In its non-aggravating form, the maximum penalty of committing a crime that fulfils the necessary elements of a criminal offence under sections 206 and 207 is three years' imprisonment.

[244] Subsection 406(1) of the Penal Code.

[245] Subsection 406(2) of the Penal Code.

[246] If the same act is committed by a legal person, the maximum amount of pecuniary punishment under the Penal Code is EUR 16,000,000. See subsection 44(8) of the Penal Code.

[247] National Strategy for Critical Infrastructure Protection – German CIP Strategy 2009; Cybersecurity Strategy for Germany, 2011.

[248] UP KRITIS Public-Private Partnership for Critical Infrastructure Protection, Basis and Goals, 2014.

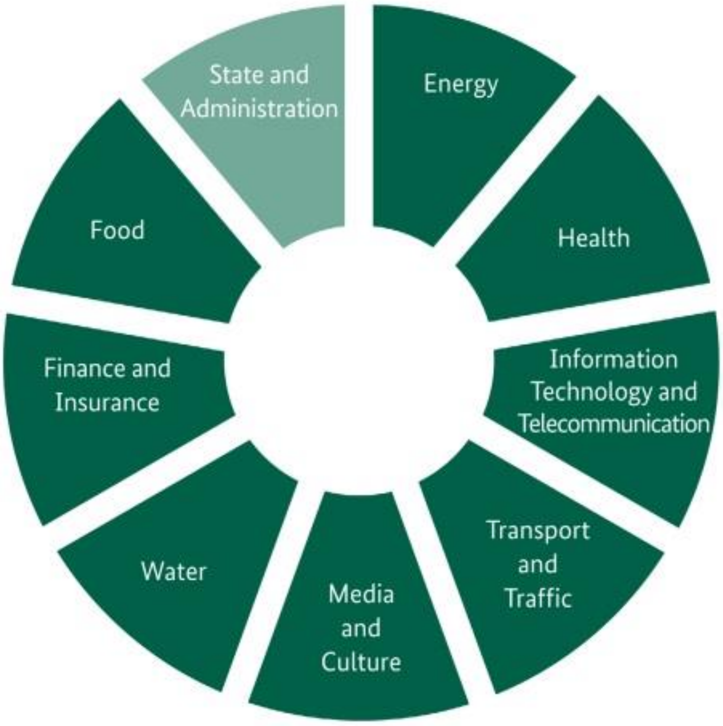


Fig. 1: The sectors of critical infrastructure in Germany

The German CIP Strategy is guided by the principle of joint action by the state, society, and business/industry. The state co-operates in partnership with other public and private actors in developing analyses and protection concepts. Either primarily as a moderator or - if required - by rulemaking, the state regulates the measures for safeguarding and securing the overall system and the system procedural flows. A look at the ownership structure of the critical infrastructure industry in Germany shows that, as a rule, the various infrastructures are not state-owned facilities but that the majority of them are operated and controlled by private enterprises – part of which were privatized only recently. Increasingly, the same applies to the many and various public infrastructure services provided at the local government level, which are being delivered more and more by private-sector enterprises. As a result of this tendency towards private ownership, the responsibility for the security, reliability and availability of such infrastructure is seen as falling on the shoulders of the private sector or, at least, is seen as a shared responsibility of the private sector and the state. As is stated in the German CIP Strategy of 2009, the state (and public authorities) primarily sees itself responsible for making provisions and – “at the most” – safeguarding and controlling the supply of goods and services in times of crisis when regular market mechanisms no longer function. The implementation of infrastructure protection measures for now is based on voluntary action, although that may change now the IT Security Act has been enacted.

Relevant Actors

In Germany critical infrastructure protection is a task performed jointly by public and private actors. The following are the most relevant actors involved in the governance of critical infrastructures protection:

- The Federal Ministry of the Interior (Federal MOI) is responsible for internal security in Germany and provides inter-departmental co-ordination of the central national-level CIP measures. Authorities within the MOI's that develop threat assessments, analyses and protection concepts are the BBK, BSI, BKA and THW (each of these abbreviations is subsequently explained).
- The Federal Office of Civil Protection and Disaster Assistance (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK) performs the tasks of civil protection and disaster relief. It develops preventive measures and policies to protect the population in emergencies and is responsible for diverse projects focusing on the protection of critical infrastructures.
- The Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) is the central IT security service provider of the German Federal Government and is therefore responsible for the protection of critical information infrastructures at the federal level. The proposed IT Security Act would strengthen the (already central) role of the BSI in regard to critical infrastructure protection.
- The Federal Criminal Police Office (Bundeskriminalamt, BKA) works together with the other agencies and includes the Cybercrime Centre.
- Agency for Technical Assistance (Bundesanstalt Technisches Hilfswerk, THW): With its specialized sections infrastructure, electric power, lighting, water damage / pumps, drinking water and leadership and communication, the THW provides emergency technical assistance to maintain critical infrastructure.
- The Federal Network Agency (Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway – Bundesnetzagentur, BnetzA) is Germany's regulatory authority for the electricity, gas, telecommunications, postal and rail markets. Since 2011, it has also taken on responsibility for implementing the Grid Expansion Acceleration Act (NABEG).
- The National Cyber Security Council and National Cyber Defence Centre.
- UP KRITIS[249] is a public-private co-operation between operators of critical infrastructures (CIP), their associations and the relevant state bodies. It is one example of a voluntary action in Germany. The aim of the cooperation is to maintain the supply of critical infrastructure services in Germany. The ultimate objective of the CIP is to maintain the supply of services of critical infrastructures in Germany. The office is located at the BSI.

[249] A study on the identification of critical processes and their IT dependencies was conducted by UP KRITIS in 2012; critical processes were identified for selected sectors and an overview of their complex dependencies was provided.

- CERTs: CERT-Bund (Computer Emergency Response Team for federal agencies) is the central point of contact for preventive and reactive measures regarding security-related computer incidents and falls under the authority of the Federal Ministry of the Interior. (See also Chapter 3)
- Providers of critical infrastructures are the companies and organisations who own these infrastructures and whose primary concern is to ensure their secure operation. These include, for example, energy suppliers or transport companies.
- Federal States (Bundesländer) - The 16 individual states within Germany are responsible for the civil protection within their own state. Thereby, diverse connections are also established with the respective local Critical Infrastructures.

Regulatory Framework

Regulation of Prevention

The Energy Industry Act[250]

The EIA regulates the provision of energy and power supply companies on a general level, thus, not limited to cybersecurity incidents and attacks. Privately organized power supply companies are under the legal obligation to operate a secure, reliable and high-performance supply network. Compliance with the (statutory) requirements is controlled by the industry's associations on the basis of the Energy Industry Act and, on the government side, by the Federal Network Agency (Bundesnetzagentur - BNetzA), especially by means of technical checks and monitoring reports. The EIA regulates the "Security and Reliability of Energy Supply" in part 6 – sections 49-53b.

Section 49 sets the requirements for power plants and states that power plants shall be constructed and operated to guarantee technical safety; they must comply with the technical rules of the technical-scientific association (Verband der Elektrotechnik, Elektronik und Informationstechnik). Section 49 also states that the Federal Network Agency (die Bundesnetzagentur) sets out the principles and procedures for the introduction of technical safety rules, while respecting the principles of the DIN (Deutsches Institut für Normung e. V. – the German agency for standardisation). The Federal Ministry of Economy and Energy (Bundesministerium für Wirtschaft und Energie) is authorized to guarantee the technical security of the technical and operational flexibility of energy systems (power plants, but also e.g. charging stations) through regulation of, in particular:

- the requirements of technical security of these systems, its construction and operation;
- the administrative procedures for ensuring the requirements above: (a) where to report establishment/modification of such facilities, (b) documents that need to be presented, (c) setting periods between the tests and the commencement of operation of such facilities (operation may only begin after certain periods following the tests);

[250] Act on the Supply of Electricity and Gas; Gesetz über die Elektrizitäts- und Gasversorgung – Energiewirtschaftsgesetz, 2005.

- checks and inspections of power plants to be carried out by officially recognised experts and rules of procedure to determine such experts;
- the establishment of administrative powers, particularly the power to prohibit construction and operation of power plants, if the project does not meet prescribed requirements;
- the information that the competent authority may require from power plant operators.

The competent authority on a state level can ensure compliance with technical security requirements in individual cases. The operator of the power plant can request the authority competent under state law for information on required technical and economic conditions. The persons authorized by the competent authority under state law with the supervision are entitled to enter business premises and facilities of power plant operators in order to carry out audits and view business and operational documents. Section 50 regulates securing energy supplies and states that the Federal Ministry of Economy and Energy is authorised to secure energy supply by regulating:

- the obligations of power companies and producers of electricity with the capacity of at least 100 megawatts to constantly have supplies of petroleum, coal or other fossil fuels in stock which are necessary to meet their required production of electricity for the next 30 days; and
- the exemptions from such obligations.

Section 51 regulates monitoring the security of supply:

- the Federal Ministry of Economy and Energy carries out the monitoring of security of supply in the field of grid-bound supply of electricity;
- the monitoring referred to in paragraph 1 must specify the relationship between supply and demand in the domestic market, the expected future demand and available supplies, and related planning and building of additional capacity, the quality and level of network maintenance, an analysis of network defects as well as measures to cover peak demand and to deal with shortfalls of one or more suppliers.

Civil Protection and Disaster Assistance Law[251]

Section 18 regulates the cooperation of Federal and State governments, stating that the Federal government with the cooperation of the German Federal States (Länder) creates a nationwide risk analysis for civil protection. The Federal Ministry of the Interior is responsible for the notification of the results of such a risk analysis (from 2010 onwards) to the German Parliament. The Federal government also advises and supports the Länder in regard to their responsibilities in protecting critical infrastructure. In consultation with the Länder, the Federal government develops standards and frameworks for civil protection, which serve as recommendations for the federal states regarding their tasks in the area of civil protection, provided that an effective cooperation of the

[251] Zivilschutz- und Katastrophenhilfegesetz; ZSKG.

authorities responsible for civil protection, in particular in the case of natural disaster and serious accidents, takes place.[252]

The Safety Assessment Act (1994) and Regulation of the Ministry of the Interior for the Material and Organisational Protection of Classified Information (2006)

Pursuant to the Safety Assessment Act 1994[253] the Regulation for the Material and Organisational Protection of Classified Information 2006 maps various security practices to assigned classification levels. These levels are set out in Paragraph 4 of the act and are assigned according to the level of risk involved in disclosing the classified information.[254]

IT Security Act (2015)[255]

An interesting, recent development in regard to protection of critical infrastructure is the newly adopted IT Security Act, which had its first hearing before the German Parliament in March 2015 and came into force in July 2015. The IT Security Act is part of the Federal Government's "Digital Agenda 2014-2017" and stipulates a binding minimum with respect to IT security standards for critical infrastructures. The IT security law is one of the first concrete results in implementing the Digital Agenda of the Federal Government. The draft Act debated in Parliament in March was strongly criticised as leading to modest provisions concerning the requirements for IT security of critical infrastructures.

The draft law defined requirements for the IT security of critical infrastructures, that is, those systems that provide critical services, such as electricity. The proposed Act required operators of critical infrastructures to meet minimum standards for IT security and to report significant IT security incidents to the BSI, which would analyse the information and make the results available to operators of critical infrastructures to help them improve their protection. To improve IT security on the Internet, the proposed law also contained stricter requirements for providers of telecommunications and telemedia services (especially website operators), which would have to offer state-of-the-art security. Telecommunications companies would also have to warn their customers if they noticed that a customer’s connection was being misused. The law would give a

[252] Art. 18 – Zusammenarbeit von Bund und Ländern:
(1) Der Bund erstellt im Zusammenwirken mit den Ländern eine bundesweite Risikoanalyse für den Zivilschutz. Das Bundesministerium des Innern unterrichtet den Deutschen Bundestag über die Ergebnisse der Risikoanalyse nach Satz 1 ab 2010 jährlich. Im Jahr ihrer Fertigstellung unterrichtet es den Deutschen Bundestag darüber hinaus über die von der Schutzkommission erstellten Gefahrenberichte.
(2) Der Bund berät und unterstützt die Länder im Rahmen seiner Zuständigkeiten beim Schutz kritischer Infrastrukturen.
(3) Im Benehmen mit den Ländern entwickelt der Bund Standards und Rahmenkonzepte für den Zivilschutz, die den Ländern zugleich als Empfehlungen für ihre Aufgaben im Bereich des Katastrophenschutzes dienen, sofern diese für ein effektives gesamtstaatliches Zusammenwirken der für den Katastrophenschutz zuständigen Behörden auch bei Naturkatastrophen und besonders schweren Unglücksfällen erforderlich sind.

[253] www.gesetze-im-internet.de/bundesrecht/s_g/gesamt.pdf.

[254] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_germany.pdf.

[255] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme IT-Sicherheitsgesetz. Description of the Act is based on the Draft Act that was debated in Parliament in March 2015; http://www.bakermckenzie.com/files/Publication/0a9affcd-4af1-48b1-af03-2622352c61b4/Presentation/PublicationAttachment/a5982c90-8b61-4119-8752-33b6b67a3086/al_germany_itsecurityact_aug14.pdf; the newly adopted Act is available here:http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1368.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1438877953289.

greater role to the BSI and emphasize its increased significance as central agency for IT security by expanding its advisory function. In order to make the security of IT products more transparent for customers, the BSI would be authorized to test the security of IT products and systems currently on the market and publish the results as needed. The proposed Act would also expand the authority of the Federal Criminal Police Office to investigate computer-related crime, in particular hacker attacks on federal IT systems.

The adopted Act, however, requires only that:

- operators of critical infrastructures ensure the provision of its major IT services required by IT to the prior art and appropriate - unless other special arrangements are in place - to make this safety check at least every two years;
- operators report to BSI significant IT security incidents;
- the obligation to report significant IT security incidents initially applies only to the operators of nuclear power plants and telecommunications companies; mandatory reporting of significant IT security incidents for other critical infrastructure operators will apply only after the adoption of the ordinance (Rechtsverordnung), which will determine which companies are subject to the provisions of the Act; the ordinance is currently being prepared by the Ministry of the Interior (the ordinance will specify the law and determine which companies will, in the legal sense, belong to the critical infrastructure).

A separate ordinance with specific rules for critical infrastructure was not planned by the draft Act. The request for a clearer definition of critical infrastructure by several industry associations was taken into account, leading to the preparation of a governmental ordinance.

Pursuant to the IT Security Act, the Act on the Federal Office for Information Security (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, 2009) was also amended (in July 2015) to broaden its scope to include critical infrastructures. The actual scope of installations and facilities covered, however, will be determined in the ordinance being prepared. The ordinance will establish measurable criteria, such as the market share of the supply of a particular region with a certain power, determining critical infrastructure in a legal sense. Other criticism, such as the increased role and power of the BSI – becoming a central office in regard to critical infrastructure protection (falling under the Federal Ministry of the Interior), which has been associated (the BSI) with the development of the "State Trojan", malware used by German law enforcement, have been disregarded. Nevertheless, if the BSI is to become the central office regarding CIP, among other matters checking the security of IT products and services, the independence of the BSI needs to be assured.

Regulation of Incident Management

EIA (2005)

Section 52 regulates the announcements of disruptions in supply and states that power plant operators are obliged to annually report to the BnetzA all supply disruptions that occurred in the last calendar year in their network. They must report the time and duration, extent and cause of the supply disruption and set out measures to avoid future supply disruptions. Facilities with national impact have immediate reporting duties. Section 53b regulates the overall system registry (regulatory power) and states that in order to guarantee the security of supply and safe operation of energy systems the Federal Ministry of Economy and Energy can regulate:

- the establishment of a directory by the Federal Network Agency containing e.g. plants for production and storage of electricity;
- the design of the system registry, in particular: (a) the information to be transmitted (location of the plant, energy sources used, capacity of the plant, technical characteristics of the plant, information about remote control capability of the system, information about the power grid to which the plant is connected), (b) who to communicate the information to, (c) requirements for the data transmission deadlines and the type, format and the scope of data transmitted, (d) comparison with data from other registers, (e) performance of duties of the asset register;
- reporting duties of the operator regarding installations requiring approval by the competent licensing authority;
- the nature and extent of the disclosure of data to network operators and third parties;
- the scope of data to be published in compliance with the data protection requirements.

IT Security Act (2015)[256]

The draft Act envisioned strengthened IT security obligations of telecommunications and telemedia companies as well as operators of critical infrastructures. According to the Act as it was adopted, these obligations, at least before the special ordinance defining critical infrastructure and obligations more specifically is adopted, apply only to operators of nuclear power plants and telecommunications companies. In addition to already applicable obligations:

- providers of publicly available telecommunications services and operators of public telecommunication networks are obligated to notify the Federal Network Agency, without undue delay, of serious security incidents of which they become aware of and which may lead to unlawful access to user systems or disrupts its availability (this is in addition to existing notification obligations in cases of a personal data breach or security breach);
- providers of publicly available telecommunication services are obligated to notify users of known disruptions caused by the users' data processing systems and to provide users with information on appropriate, effective and accessible technical measures to detect and remedy such disruptions;
- telemedia service providers are obligated to provide secure authorization methods for personalized telemedia services and, where technically feasible and reasonable, take measures to ensure that unlawful access to data processing and telecommunication system is prevented;

[256] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme IT-Sicherheitsgesetz.

- telecommunications and telemedia providers shall be entitled to use their customers' data to protect their customers and to resolve disruptions.

Similar obligations apply to operators of nuclear power plants.

Act on the Federal Office for Information Security (2009)[257]

Germany does not have a national incident management structure in place for responding to cybersecurity incidents. The Act on the Federal Office for Information Security 2009 gives the BSI the authority to act as the national authority for information security. The act does not outline a general incident management structure, nor specific practices related to cybersecurity.[258] The Act requires federal authorities to report cybersecurity incidents to the Federal Office of Information Security upon detection. An amendment to the Act came into force in July 2015, strengthening the mandatory reporting requirements covering telecommunication service providers and entities engaged with critical infrastructure. Sub-section a) and b) were added to section 8 in regard to critical infrastructure.

Section 8a Security of Information Technology Critical Infrastructure indicates that operators of critical infrastructures are required, no later than two years after the entry into force of the Ordinance pursuant to § 10 paragraph 1, to apply appropriate organizational and technical measures to avoid disruption of the availability, integrity, authenticity and confidentiality of their essential information technology critical infrastructure systems, components or processes of their functioning. The state of the art of the technology should be taken into account. Organisational and technical measures are appropriate when the costs for applicants are not disproportionate to the consequences of a failure or deterioration of the affected critical infrastructure.

Operators of critical infrastructure and their inter-branch organizations can propose industry-specific safety standards to ensure the requirements of paragraph 1. The Federal Office firmly tests whether these proposals are appropriate for ensuring the requirements of paragraph 1. The test is conducted in consultation with the Federal Office for Civil Protection and Disaster Assistance, the relevant supervisory authority of the Federation or the other competent supervisory authority. The operators of critical infrastructure should appropriately demonstrate compliance with the requirements in accordance with paragraph 1at least once every two years. This can be done by security audits, inspections or certifications. The operator shall report to the Federal Office a list of audits carried out, examinations or certifications including the safety deficiencies uncovered by them.

In regard to the security deficiencies the Federal Office may demand: the transmission of the entire audit, examination or certification results and the removal of safety deficiencies in consultation with the relevant supervisory authority of the Federation or in consultation with the other competent authority. In regard to the design of the procedure of security audits, examinations and certifications and the requirements for the manner of execution, based on the acquired

[257] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik.

[258] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_germany.pdf.

evidence, the Office may set technical and organizational requirements after consultation with the representatives of the operator and trade associations concerned.

Section 8b regulates the tasks of the Central Office for Security in Information Technology Critical Infrastructures, which the Federal Office for Information Security as the reporting office for operators of critical infrastructures in matters of Security in Information Technology. More specific obligations for the providers and the Federal Office will be regulated in the ordinance.

Regulation of Repression

The German Criminal Code[259] regulates the interference with and prevention of provision of certain critical infrastructure services, such as electricity, in section 316b (disruption of the provision of telecommunication services is, however, regulated in section 317).

Section 316b – Disruption of public services

> (1) Whosoever prevents or interferes with the operation of enterprises or facilities which serve the public provision of postal service or public transport; a facility which serves the public provision of water, light, heat or power or an enterprise which serves the vital needs of the population; or an installation or a facility serving public order and safety by destroying, damaging, removing, altering or rendering unusable an object used in its operation or taps electrical power intended for its operation shall be liable to imprisonment not exceeding five years or a fine.
>
> (2) The attempt shall be punishable.
>
> (3) In especially serious cases the penalty shall be imprisonment from six months to ten years. An especially serious case typically occurs if by the offence the offender disrupts the provision of vital goods to the population, in particular water, light, heat or power.[260]

Section 317 – Disruption of telecommunications facilities

> (1) Whosoever prevents or endangers the operation of a telecommunications facility which serves public purposes by destroying, damaging, removing, altering or rendering unusable an object which serves its operation, or taps electrical power intended for its operation shall be liable to imprisonment not exceeding five years or a fine.
>
> (2) The attempt shall be punishable.
>
> (3) Whosoever commits the offence negligently shall be liable to imprisonment not exceeding one year or a fine.[261]

[259] Strafgesetzbuch (StGB).

[260] Translation by Prof. Dr. Michael Bohlander, available at http://www.gesetze-im-internet.de/englisch_stgb/index.html.

[261] Idem.

4.2.4 The Netherlands

Under the 1998 Dutch Electricity Act (DEA), the Ministry of Economic Affairs is responsible for drafting an energy report at least every four years (article 2(1) DEA). After the report is finalized, it is communicated to Parliament and then published (in the 'Staatscourant', the official gazette for informing the public about legislative decisions, since 2009 this is published via internet at http://officielebekendmakingen.nl).[262] The Authority for Consumers and Markets (ACM) is the regulatory authority for the energy sector and is responsible for the implementation and supervision of the act (articles 5-9 DEA); it also develops Energy Codes (see section 4.1.3). The ACM advises the Minister of Economic Affairs on the designation of network operators, licenses for suppliers to small consumers, tariffs and tariff structures of transmission- and system services, and delivery rates[263] and determines the conditions for the free market, including free access to the electricity network under equal conditions.[264] Every two years, the ACM assesses whether network operators sufficiently and efficiently provide the total needs of transport.[265] The ACM works together with institutions from other EU Member States that are responsible for electricity regulation based on their national laws, and with 'The Agency' as meant by article 1(1) of Regulation 713/2009, which is an agency for the cooperation amongst energy regulators. The ACM also works together with the national actors outlined in the next section.

In 2013, the Dutch government presented the Dutch "National Cyber Security Strategy 2".[266] It distinguishes five strategic goals: 1. the Netherlands is resilient against cyber attacks and protects its vital interests in the cyber domain. 2. The Netherlands deals with cyber criminality. 3. The Netherlands invests in secure and privacy-protecting ICT products and services. 4. The Netherlands forges coalitions for freedom, security and peace in the cyber domain and 5. The Netherlands has at its disposal sufficient cyber security knowledge and experience and invests in ICT-innovation in order to achieve its cyber security goals. The government regularly reports to the parliament about the progress made with the implementation of the strategy. The last progress letter dates from December 2014.[267] About the energy sector, this report mentions that Tennet and Shell have started collaboration for charting vulnerabilities, dependencies and counter measures in the chain of energy provisioning. Furthermore, it announces that the Computer Crime III bill will be introduced in parliament in the first half of 2015.[268]

Relevant Actors

In addition to the Ministry of Economic Affairs and ACM, the following actors are relevant to the governance of energy infrastructures:

[262] The Minister of Security and Justice also played an active role during recent power outages in the North of the Netherlands.

[263] https://www.acm.nl/nl/onderwerpen/energie/elektricitieit/

[264] Idem.

[265] Idem.

[266] Available here: https://www.rijksoverheid.nl/documenten/rapporten/2013/10/28/nationale-cyber-security-strategie-2

[267] Available here: https://www.rijksoverheid.nl/documenten/kamerstukken/2014/12/19/tk-voortgangsbrief-realisatie-werkprogramma-nationale-cyber-security-strategie-2

[268] In May 2015, a public consultation was started. See https://www.internetconsultatie.nl/computercriminaliteit

- The Provincial Council is responsible for the construction or expansion of a production plant for the generation of renewable electricity (art. 9e (1) DEA); this falls within the scope of the Spatial Planning Act (Wet ruimtelijke ordening).
- The Provincial Executive coordinates the preparation and publication of decisions concerning the construction or expansion of a production plant as meant in art. 9e DEA.
- An electricity producer is an organizational unit that deals with the generation of electricity (art. 1(1) g DEA). Large producers in the Netherlands are: NUON, Essent, Elektrabel, Intergen, Delta, Eneco and EON.[269] An electricity supplier is an organizational unit that deals with the supply of electricity (to the consumers). According to article 9h(1) DEA, a producer who produces electricity with a direct line to consumers, reports to the ACM once opening that direct line.
- The network operator (grid) is concerned with the physical transport of electricity and must ensure the safety and reliability of the networks and the transport of electricity on those networks in the most effective manner (art. 16(1)(b) DEA). The network operator must also build, renew and extend the nets and develops an emergency plan every five years that must be approved by the Minister of Economic Affairs.[270] The network operator keeps record of quality indicators for electricity transmission (art. 19a DEA) and ensures that interruptions in the electricity transport are easily reported, recorded and made public (art. 19e DEA). TenneT is the administrator/operator of the Dutch national grid.[271] Regional network operators administrate the high voltage distribution nets and the low voltage net/grid.
- Program Managers buy the electrical power from the suppliers and have an obligation to deliver. Each party that has one or more connections to a network is responsible (as a Program Manager) for that connection. Program Managers indicate how much electricity they expect to supply to the grid and the expected take away/withdrawal from the network. The sum of all expected supplies and withdrawals is called an Energy Program; these are published to TenneT daily. The ones responsible for the measurement must measure the actual production or actual consumption every day. The summed measurements must be passed to TenneT, who will settle the difference between what is submitted and what has been measured. If a Program Manager does not adhere to the Energy Program that results in an imbalance which has financial consequences.[272]
- Metering companies measure actual consumption in accordance with the Metering Code *(*Meetcode*)*. Each party connected to the grid is responsible for timely and proper measuring of its electricity exchange with the grid, as well as timely and proper disclosure of this information to its network operator. The affiliate is free to perform this measurement itself,

[269] Useful website: http://www.energie-nederland.nl/aangesloten-energiebedrijven/

[270] The Minister may issue a direction in the context of protection of networks against possible external influences (art. 16da).

[271] http://www.tennet.eu/nl/nl/over-tennet.html

[272] http://www.tennet.eu/nl/nl/klanten/diensten/syteemdiensten/programmaverantwoordelijkheid.html

provided it is recognized as responsible for metering by TenneT. Affiliates may also outsource their measuring responsibility to a third party who has been recognized as metering responsible. The tasks include placing meters, maintenance and meter-by-meter readings.

- Representative organizations mediate some interactions between different actors. Two key representative organizations are Netbeheer Nederland, the branch organization of network operators (http://www.netbeheernederland.nl/) and NEDU/EDSN, the vereniging Nederlandse Energie Data Uitwisseling/Energy Data Services Netherlands (http://www.edsn.nl/). These organizations are important because they can also submit a proposal to the ACM to change the aforementioned Energy Codes.

Regulatory Framework

Regulation of Prevention

The Dutch Electricity Act (DEA) 1998

The net manager – entity entrusted with the physical transport of electricity – must guarantee the safety and reliability of the transport nets for electricity in the most efficient way possible (art. 16(1) sub b DEA). The net manager must protect its nets against possible external forces (art. 16(1) sub q DEA). The net manager draws up a calamities plan at least once in every five years and sends this plan for approval to the Minister of Economic Affairs (art. 16d(1) DEA).

A concept for a new electricity and gas bill has been drawn up and laid open for an Internet consultation.[273] Relevant obligations from the DEA return in this bill, inter alia the obligation to protect against external forces returns (art. 5.4(2) Electricity and Gas Bill). In the concept Explanatory Memorandum, a cyber-attack is explicitly mentioned as an example of an external force.[274]

The Dutch Independent Net Management Act[275]

This Act stipulates that net-managers may not belong to the same concern as producers of, traders in and retailers of electricity. This unbundling is mainly inspired by economic considerations and the implications for security do not appear to have played an appreciable role. Nonetheless, the unbundling of previously integrated firms may lead to security responsibilities becoming distributed over multiple parties, which (theoretically, at least) may lead to a greater need for coordination in the field of security. Apart from this concern, unbundling may also have an advantage in security terms. It may be easier to contain problems (to one part of the network) and some parts of the network may temporarily take over the function of other parts that are stricken down as a consequence of a security breach.

[273] 'Concept Wetsvoorstel Stroom' http://www.vemw.nl/~/media/VEMW/Downloads/Public/Homepage%20homeslider/MvT%20Wetsvoorstel%20STROOM%20versie%202.ashx

[274] Concept Explanatory memorandum, p. 80, available at: http://www.vemw.nl/~/media/VEMW/Downloads/Public/Homepage%20homeslider/MvT%20Wetsvoorstel%20STROOM%20versie%202.ashx

[275] Wet onafhankelijk Netbeheer.

ACM Energy Codes

As mentioned above, the ACM sets the so-called Energy Codes. These are regulations that contain rules that hold between net managers and users of the gas- or electricity net. Producers of energy are for example users of the net. One of the electricity codes is the cooperation regulation. Its tenth article, entitled 'Calamities (terrorist attacks, natural disasters, war etc)' states that it is every Net Manager's responsibility to have a calamity plan. If and to the extent necessary net managers will exchange their individual plans, discuss them and attune them to each other. If necessary, all net managers involved will draw up common plans.

Regulation of Incident Management

Dutch Concept Bill on Cyber Security Data Processing and Reporting of Incidents[276]

In early 2015, the Dutch government published a concept bill on the reporting of cybersecurity incidents and an invitation to any interested party to make its views known in the accompanying Internet consultation. According to the published bill, the duty to report incidents rests on certain providers of products or services that are pointed out in a Ministerial Decree. The Ministerial Decree will point out parties in the following sectors: electricity, gas, drinking water, telecommunication, government (including see and river water management) and transport (such as the main ports, Rotterdam and Schiphol). Concretely, it will concern vital providers, such as energy network managers, drinking water companies, telecom companies, managers of waterworks or banks.

An incident must be reported to the Minister of Security and Justice. Any incident report will be processed by the Nationaal Cyber Security Centrum (NCSC), which functions under responsibility of the Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). A report enables NCSC to offer support to the affected provider and to warn other providers. The ultimate goal is to make an assessment of the risk of societal disruption and to prevent such disruption, or at least to minimize it as much as is possible. The affected organizations are not obliged to report each ICT-incident to the NCSC. The duty to report only applies to incidents where the availability or reliability of the pertinent product or service is or can be interrupted to a serious extent. With this bill, the Dutch government anticipates the adoption of the proposal for a Council Directive 2013/0027 concerning measures to ensure a high common level of network and information security across the Union, which regulates incident reporting and the handling of the reported data as well.

The Dutch Electricity Act (DEA)

The Minister of Economic Affairs can instruct the net manager with respect to the protection of the nets against external forces (art. 16da DEA). The net manager facilitates easier reporting, registering and publishing with regard to interruptions in the transportation of electricity (art. 19e DEA). A concept for a new electricity and gas bill has been drawn up and made available for

[276] http://www.Internetconsultatie.nl/cybersecurity

Internet consultation.[277] Relevant provisions from the DEA return in this bill, inter alia the Minister's power to give instructions relating to protection against external forces returns (art. 10.5 Electricity and Gas Bill). In the concept Explanatory Memorandum, a new technical development in cyber criminality is explicitly mentioned as an example of a concrete threat that may lead the Minister to give an instruction.[278]

Regulation of Repression

Articles 161bis, 161ter, and 351bis Dutch Criminal Code concern crimes that disrupt electricity provision.

> Art. 161bis: He who intentionally destroys, damages, makes unusable or causes disruption in the progress or functioning of any electricity work or who frustrates any safety measure taken with respect to such work, shall be punished (1) with imprisonment of at most one year or a fine of the fifth category if as a consequence of it, impediment or complication of electricity delivery for the common good arises, (2) with imprisonment of at most six years or a fine of the fifth category if as a consequence of it, common danger to goods must be feared, (3) with imprisonment of at most nine years or a fine of the fifth category if as a consequence of it, lethal danger to another must be feared (3) with imprisonment of at most fifteen years or a fine of the fifth category if as a consequence of it, lethal danger to another must be feared and the act has caused somebody's death.
>
> Art. 161ter: He who is to blame that any electricity work is destroyed, damaged, made unusable or that disruption in the progress or functioning of it is caused or that any safety measure taken with respect to such a work is frustrated, shall be punished (1) with imprisonment of at most six months or a fine of the fourth category if as a consequence of it impediment or complication of electricity delivery for the common good arises, or if as a consequence of it, common danger to goods must be feared, (2) with imprisonment of at most one year or a fine of the fourth category if as a consequence of it, lethal danger to another arises (3) with imprisonment of at most two years or a fine of the fourth category if the act has caused somebody's death.
>
> Art. 351: He who intentionally and without right destroys, damages, makes unusable, causes to be out of order or lost, railway or electricity works, automated works or works for telecommunication, dams, works for drainage, gas or water lines or sewage, for as far as these works are used for the common good, or goods or works for the defense of the country, will be punished with imprisonment of at most three years or a fine of the fourth category.
>
> Art. 351bis: He who is to blame that any good or work meant in the previous article is destroyed, damaged, made unusable or caused to be out of order or lost will be punished with imprisonment of at most one month or a fine of the second category.

[277] 'Concept Wetsvoorstel Stroom' http://www.vemw.nl/~/media/VEMW/Downloads/Public/Homepage%20homeslider/MvT%20Wetsvoorstel%20STROOM%20versie%202.ashx

[278] Concept Explanatory memorandum, p. 124, available at: http://www.vemw.nl/~/media/VEMW/Downloads/Public/Homepage%20homeslider/MvT%20Wetsvoorstel%20STROOM%20versie%202.ashx

Moreover, the general provisions on data interference (art. 350a DCC) and system interference (particularly botnet attacks, art. 138b DCC) include an aggravated circumstance if the crime is targeted at computers belonging to vital infrastructures, with a maximum punishment of five years' imprisonment or fine of the fourth category (art. 138b(3), 350a(2) DCC).

Because these crimes express the vital importance that electricity provision has for society, they are formulated in a technology-neutral way with respect to the means that a perpetrator uses in rendering an electricity work unusable or causing impediments to its functioning. Therefore, they are usable if the crime is committed by way of a cyber-attack. The maximum punishment appears to be rather low, especially it the effect is merely an interruption in electricity provision. This has effects on the investigatory powers that can be used to track down the perpetrators, since the most relevant investigation powers can only be used for crimes that have a maximum punishment of at least four years (art 67 Dutch Code of Criminal Procedure). However, art. 351 is also explicitly mentioned in art. 67 Code of Criminal Procedure, and thus allows the relevant investigation powers to be used, so that cyberattacks on electricity works can investigated under art. 351. Moreover, if the attack resulted in common danger to goods (not necessarily actually damaging goods, but providing a considerable risk that goods with a public function would be damaged), also investigation under art. 161bis(2) is possible.

4.2.5 United Kingdom

Following the privatization and the public/private partnership agreements that concerned the water, energy (gas and electricity) and telecommunications sectors in the 1980s and 1990s, a large part of the UK National Infrastructures (CNI) – including the electrical grid – is privately owned and operated. Public authorities set both the framework within which CNI asset owners deliver their services and the protection measures and security controls they have to implement.

CNI are increasingly interconnected and reliant on ICT in their functioning.[279] Modern industrial control systems (ICSs) and SCADA systems are generally connected to the Internet and based on open standards and architectures, and therefore subject to the potential vulnerabilities that the access to the Net entails.[280] Moreover, critical infrastructures are highly interconnected and interdependent: for instance, an energy supplier's product could be transmitted through an infrastructure owned by another subject and then delivered to its users. The consequences of a successful cyber attack targeting an ICS deployed in the context of a CNI are serious, and the UK's policies appear to recognize this issue.

In 2008, the Government published the first National Risk Register for Civil Emergencies (NRR), fulfilling a promise from that year's National Security Strategy.[281] The document, which is

[279] See Paul Cornish et al., 'Cyber Security And The UK Critical Infrastructure' (Chatham House Report, 2011), p. 1.

[280] For a brief overview of recent cyberattacks targeting SCADA systems see Andrew Nicholson et al., 'SCADA security in the light of Cyber-Warfare', (2012) 31 Computers & Security, 418. See also Stewart Baker et al, 'In the crossfire: Critical infrastructure in the age of cyber war' (McAfee 2009); and Stewart Baker et al., 'In the Dark: Crucial Industries Confront Cyber Attacks' (McAfee 2011).

[281] Cabinet Office, 'National Risk Register' (2008), p. 3.

regularly updated,[282] assesses the likelihood and potential impact (i.e. the risk level) of a negative and unwarranted event, potentially involving a significant part of, or the whole nation. The NRR's approach is to a large extent holistic; it takes into account quite a large array of natural events, accidents and malicious attacks. Regarding electricity-related issues, the 2008 NRR states, "There are comprehensive plans in place for handling both a complete national outage and regional outages. In the event of a national outage (which has never occurred), and provided there had been no damage to the system, the objective would be to restore supplies throughout Great Britain within three days."[283] It also specifies that – in case of intentional and malicious attack on critical infrastructures – there are "longstanding and regularly activated major incident plans and structures are in place across government."[284] It also notably adds, "Planning for the impacts of attacks on critical infrastructure is in many cases the same as for accidents or technical failure."[285] The 2010 NRR and the 2012 update, as well as the 2013 NRR, do not contain any significant changes, but the 2015 document indicates that the NRR raised the risk level of a critical power outage following government research.[286] All nine industry sectors are interested in specific programs and general incident response procedures.

Relevant actors

The following actors are relevant to the governance of energy infrastructures:

- Centre for the Protection of National Infrastructure (CPNI) is specifically tasked with providing advice, guidance and best practices to national infrastructure**[287]** stakeholders on protective security measures. The CPNI was formed in 2007 with the merger of the National Infrastructure Security Co-ordination Centre (NISCC) and the National Security Advice Centre (NSAC).**[288]** (NISCC provided advice to companies and other bodies involved in the CNI operations, while NSAC was a unit within MI5 that provided advice on security matters.) CPNI provides operational guidance on information security, physical security and personnel security, and focuses on protecting the UK national infrastructure from espionage, terrorism and other security threats.
- National Cyber Security Programme, OCSIA and CSOC The first UK Cyber Security Strategy (2009 CSS) was launched in June 2009,[289] paving the way for the creation of the Office of Cyber Security and Information Assurance (OCSIA), a group within the Cabinet Office responsible for the UK cybersecurity policy implementation and the Cyber Security Operations Centre (CSOC), a multi-agency body tasked with national incident response coordination.

[282] In 2010, 2013, 2013 and 2015.
[283] Cabinet Office, 'National Risk Register' (2008), p. 21.
[284] Cabinet Office, 'National Risk Register' (2008), p. 26.
[285] Ibid.
[286] Cabinet Office, 'National Risk Register' (2015), p. 15.
[287] The UK national infrastructure is categorized according to 9 categories: communications, emergency services, energy, financial services, food, government, health, transport, and water. Each of those categories is then divided into sub-categories. Each category has a governmental lead, some sharing the same one.
[288] Andrew Wood, 'Resilience of the Critical National Infrastructure' (Ogres Working Paper 2008), p. 4.
[289] OCS and CSOC, 'Cyber Security Strategy of the United Kingdom – safety, security and resilience in cyber space', (Cabinet Office, June 2009).

- The Government Communications Headquarters (GCHQ) is a British intelligence and security organisation responsible for providing signals intelligence and information to the British government and armed forces.
    - CESG,[290] formerly called Communications-Electronics Security Group, is now known as the National Technical Authority for Information Assurance and situated within GCHQ., It provides information security advice, information assurance and other services (e.g. certifications, independent reviews, training etc.) to government, defence and CNI stakeholders. It plays a key role in proactively securing UK CNI from cyber attacks.
- Computer Emergency Response Teams (CERTs) also play a key role in protecting networked CNI. They are present at both the national (i.e. CERT-UK[291]) and sectoral or regional levels. The government has its own CERT (GovCertUK[292]) and private bodies – such as CNI operators, which in the UK are mostly private parties – are also actively encouraged to form their own. The responsibilities of CERT-UK include: national cybersecurity incident management, support to critical national infrastructure companies when handling incidents, promoting cybersecurity situational awareness across industry, academia and the public sector and providing the single international point of contact for co-ordination and collaboration with other national CERTs.[293] CERT-UK also leads the Cyber-security Information Sharing Partnership (CiSP[294]), a platform where public and private stakeholders can share information and analysis regarding threats and vulnerabilities between.
- Department of Energy and Climate Change (DECC), formed in 2008, is a ministerial department responsible for energy policies in the UK and the leading department for the energy infrastructure sector. Its responsibilities[295] include energy security – ensuring UK businesses and households have secure supplies of energy[296] and managing the UK's energy legacy safely, securely and cost effectively.[297] The DECC works with 9 agencies and public bodies: Ofgem (the Office of Gas and Electricity Markets), Oil and Gas Authority, Civil Nuclear Police Authority, Coal Authority, Committee on climate change, Nuclear Decommissioning Authority, Committee on Radioactive Waste Management, Fuel Poverty Advisory Group and the Nuclear Liabilities Financing Assurance Board.
- The Civil Contingencies Secretariat (CCS) is a governmental office within the Cabinet Office tasked with fostering the UK's contingency management and response capabilities, providing

[290] CESG, https://www.cesg.gov.uk/, last access May 2015.

[291] CERT-UK, https://www.cert.gov.uk/, last access May 2015.
See also Cabinet Office and The Rt Hon Lord Maude, 'UK launches first national CERT' (2014), https://www.gov.uk/government/news/uk-launches-first-national-cert, last access May 2015.

[292] CESG, https://www.cesg.gov.uk/PolicyGuidance/GovCertUK/Pages/index.aspx, last access May 2015.

[293] CERT-UK, https://www.cert.gov.uk/what-we-do/, last access May 2015.

[294] CERT-UK, https://www.cert.gov.uk/cisp/, last access May 2015.

[295] DECC, 'About Us', https://www.gov.uk/government/organisations/department-of-energy-climate-change/about, last access June 2015.

[296] Ibid.

[297] Ibid.

leadership, insight and guidance to other bodies. The CCS is involved in the production of the NRA and the NRR, is responsible for emergency planning and response, and leads policing activities directed towards CNIs.[298]

Regulatory Framework

In the UK there is no single piece of legislation governing the protection of CNI from cyber attacks. There is, however, specific regulation aimed at disciplining CNI-related contingencies, albeit fragmented between sectors. In the event of a sufficiently serious electricity supply emergency, both industry[299] and government[300] are tasked with managing the incident and its consequences. Several laws that potentially apply at some stage of a cyberattack targeting a CNI tasked with the production, transmission or distribution of electrical energy are described below.

Due to the nature of this quick-scan report, and to the fragmented nature of UK criminal legislation, some more general provisions that are likely to be applicable in the event of a cyber attack targeting an electricity-related CNI (such as the ones contained in the Criminal Law Act 1977 (c.45)) are not examined. The legislation that covers the UK public bodies' Intelligence, counter-terrorism and investigatory powers, for instance, is undoubtedly to be considered when assessing the national capacity to prevent, stop and repress a cyber attack targeting a CNI. In particular, it is worth mentioning the Security Service Act[301] and the Intelligence Services Act[302], which provide a statutory basis for the UK's intelligence agencies, and the Regulation of Investigatory Powers Act,[303] which regulates the intelligence's investigative powers, along with those of other relevant public bodies. Moreover, the Counter-Terrorism Act[304] is likely to be applicable, as well; especially when the cyber attack targeting a UK CNI has physical effects.

Regulation of Prevention

Energy Act 1976

The powers foreseen in the Energy Act 1976[305] (EA76 henceforth) enable the Secretary of State for DECC to control the production, supply, acquisition and use of energy (electrical one included) in case of an "*there exists or is imminent in the United Kingdom an actual or threatened emergency affecting fuel or electricity supplies which makes it necessary in Her Majesty's opinion that the government should temporarily have at its disposal exceptional powers for controlling the sources*

[298] See University of Cambridge, Centre for Science and Policy, 'Civil Contingencies Secretariat (CCS), Cabinet Office', http://www.csap.cam.ac.uk/organisations/civil-contingencies-secretariat/, last access May 2015.

[299] "*The gas and electricity companies are responsible for the practical and operational management of an incident in order to ensure that the situation is contained, managed safely and supply effectively restored. The companies have well established plans and procedures in place to achieve this, which can range from the management of a moderate supply deficit to the management of a major loss of gas supplies impacting on domestic consumers or restoration of electricity supplies from a national shut down*": DECC, 'National Emergency Plan – Downstream Gas & Electricity', (Version 15, November 2014), p. 7.

[300] The Department of Energy & Climate Change (DECC) being the UK Competent Authority and Lead Government Department in case of electricity-related emergencies.

[301] Security Service Act 1989 (c 5).

[302] Intelligence Services Act 1994 (c. 13).

[303] Regulation of Investigatory Powers Act 2000 (c.23).

[304] Counter-Terrorism Act 2008 (c. 28).

[305] The Energy Act 1976 (c. 76).

and availability of energy."[306] The aforementioned exceptional powers,[307] which are crucial in managing and preventing the potential effects of a cyber attack targeting UK electricity-related CNIs, are granted by an Order in Council *ex* section 3 EA76. In particular, the Secretary of State can regulate or prohibit the production, supply, acquisition or use of electricity, but only where it seems desirable in order to conserve energy.[308] The Secretary of State, when an aforementioned Order in Council *ex* section 3 is in place, can also give directions to any subject involved in the production, supply, or usage of electricity.

Electricity Act 1989

The Electricity Act 1989 (EA89) enacted the final privatisation instances of the UK's electricity market, established a licensing program, and gave birth to the Office of Electricity Regulation (OFFER), now known as the Office of Gas and Electricity Markets (OFGEM).

In preventing the potential damages deriving from a successful cyber attack targeting the UK, the licensing conditions imposed to undertakings performing electricity production, transmission and distribution activities is important. The EA89 confers the Secretary of State the capacity to issue broad Directions to both power stations and transmission operators. The Fuel Security Code[309] in particular provides an administrative structure in which to frame the Secretary of State's directions, which include, for instance, setting an appropriate level of energy stock and making provisions for operators on how to use such stock. The Electricity Supply Emergency Code (ESEC) is another document likely to matter, in that it describes how the UK Government might deal with an electricity supply emergency as envisaged in the EA89 or in the Energy Act 1976. It also sets out the actions, which companies in the electricity industry should plan to take and which may be needed or required in order to deal with such an emergency.

Regulation of Incident Management

Civil Contingencies and the CCA 2004

As mentioned, the hypothetical case used as a lens to scan the UK's approach towards CNI cyber security outlines a major attack targeting electricity production and transmission facilities. Identifying the source of the CNI failure and, most likely, attributing it to a specific malicious threat actor, rather than to technical failure or negligence, could initially be difficult. In any case, the emergency deriving from a successful cyber attack targeting the UK's electrical grid or the related CNI would be dealt with as a civil contingency, disciplined by the Civil Contingencies Act 2004[310] (CCA) and by its related regulations and governmental guidance, which will be briefly outlined below. The CCA constitutes the UK's general framework for emergency planning, management and response, both from local and from a national level – defense issues, however, are excluded

[306] EA76, section 3.1 (b).
[307] i.e. the ones granted by sections 1 and 2 of the EA76.
[308] EA76, section 1.
[309] Department for Business, Enterprise & Regulatory Reform, 'The Fuel Security Code' (2007). The Fuel Security Code's provisions are incorporated by reference into licenses, have therefore the status of license condition, and are enforceable by the competent authorities.
[310] The Civil Contingencies Act 2004 (c 36).

from the scope of the act. The CCA mandates the cooperation of a range of public bodies, as well as of a number of private actors, utility companies included. Due to the extent of the powers conferred by the act and to their exceptional character, the CCA's provisions are to be considered as having a residual nature.

The CCA is composed by three parts: the first one dedicated to "*Local arrangements for Civil Protection*", which provides "*a framework that governs the planning and preparation for a wide range of post-cold war potential emergencies, including terrorist incidents, cyber-attacks and natural hazards such as flooding or extreme weather*[311]"; the second one to the government's extraordinary "*Emergency Powers*", and the last one to a number of general provisions. The CCA is completed by two schedules, the first identifying the subjects bound to respond to the contingency and the second one the amendments and repeals enacted by the CCA. Part 1, Section 1 and Part 2, Section 19 define an "emergency" as either:

a. An event or situation which threatens serious damage to human welfare in a place in the United Kingdom;
b. An event or situation which threatens serious damage to the environment of a place in the United Kingdom;
c. War, or terrorism, which threatens serious damage to the security of the United Kingdom.

"*Damage to human welfare*", in the context of the CCA, as Section 1 and 19's subsections 2 state, means only damage involving "*loss of human life, human illness or injury, homelessness, damage to property, disruption of a supply of money, food, water, energy or fuel, disruption of a system of communication, disruption of facilities for transport, or disruption of services relating to health*". The energy disruption following a successful cyber attack on UK's electrical infrastructure would therefore be considered in the scope of the CCA. Notably, a Minister of the Crown[312] may order that a specified event is to be treated as falling (or not falling) within any of paragraphs defining the concept of emergency or those specifying what "damage to human welfare" is.

The first schedule of the CCA identifies the subjects bound to respond to an emergency, framing them in two separate categories, Category 1 and Category 2 responders: the first category[313] comprises emergency and health services, as well as local authorities, while the second[314] comprises an array of entities that are likely to play a major role in case of specific emergencies (including for instance, persons holding an electricity transmission, distribution or interconnection license). Category 1 respondents bear the primary responsibility for emergency planning and response. Section 2 of the CCA specifies that both categories of respondents have a duty to assess possible future emergencies, to plan ahead and to produce the relevant advice, publishing their assessment and plans if useful to prevent the emergency, to reduce, control or mitigate the damages or to enable others to undertake the necessary actions. A Minister of the

[311] Rebecca Moosavian 'Keep Calm and Carry On: informing the public under the Civil Contingencies Act 2004', (2014) 18 The International Journal of Human Rights 178.

[312] Or, if Scotland is involved, the Scottish Ministers.

[313] CCA, Schedule 1, part 1. Category 1 responders are the 'front line', the subjects primarily tasked to respond to emergencies.

[314] CCA, Schedule 1, part 2.

Crown, in relation to a person or body listed in Part 1 of Schedule 1, or the Scottish Ministers, in relation to a person or body listed in Part 2 of Schedule 1, may issue guidance[315] or regulate the extent and the manner of the duty to assess, plan and advise foreseen in the first subsection of Section 2. It is also foreseen that a public body shall have the duty to provide advice and assistance to the public.[316]

Section 5 states that a Minister of the Crown may order a Category 1 respondent to perform a broad range[317] of functions in order to prevent the occurrence of an emergency, reduce, control or mitigate the effects of an emergency, or take other action in connection with an emergency. The provision applies to Scottish Ministers, as well; albeit with some additional limitations.[318] Where there is an urgent need to make provision of a kind that could be made by an order or by regulations under section 5(1) or 6(1), but there is insufficient time for the order or regulations to be made, the Minister is allowed make those provision by direction, instead of by order or regulation, thus having the possibility to deal with extreme urgencies.[319]

Information sharing and disclosure play also a prominent role in Part 1 of the CCA. On one hand, Section 6 allows a Minister (either of the Crown or a Scottish one) to require or permit a Category 1 respondent to disclose information on request to another respondent, be it of Category 1 or 2. On the other, Section 9 allows a Minister to require a Category 1 respondent to provide information about action taken or to explain why the person or body has not taken the action required.

Part 2 of the CCA is about government emergency powers. Section 20(1) states that "*Her Majesty may by Order in Council make emergency regulations*"; in case this is not possible without serious delay, Section 20(2) allows those emergency regulations to be taken by a Minister of the Crown. In any case, the emergency regulations shall be made by statutory instrument[320] can be taken only if the following conditions are satisfied[321]:

1. An emergency has occurred, is occurring or is about to occur;
2. It is necessary to make provision for the purpose of preventing, controlling or mitigating an aspect or effect of the emergency;
3. The need for the emergency provision is urgent.

Section 22 of the CCA, dealing with the (broad) scope of the emergency regulations, states that they "*may make any provision which the person making the regulations is satisfied is appropriate for the purpose of preventing, controlling or mitigating an aspect or effect of the emergency in respect of which the regulations are made*". The section clarifies and exemplifies the ample range of powers regulations that can be taken in case of emergency. Emergency regulations are subject to statutory limitations,[322] expire 30 days after the date on which they are made (or earlier time if

[315] See *inter alia* CAA, Section 3.
[316] See CCA, Section 4.
[317] See CCA, Section 5(4).
[318] See CCA, Section 5(5).
[319] See CCA, Sections 7 and 8.
[320] See CCA, Section 30.
[321] See CCA, Section 21(2)(3)(4).
[322] See CCA, Section 23.

specified in the regulations)[323] and are subject to parliamentary scrutiny.[324] Moreover, if a devolved administration is interested in a proposed emergency regulation, a senior minister must be consulted.[325] Coordination is ensured by the appointment of an Emergency Coordinator for each part of the UK other than England by a senior Minister of the Crown, and of a Regional Nominated Coordinator for each region interested, whose role is facilitating coordination between the actors involved.[326]

The CCA displays the integration of two different organisational structures, a C&C model and a more decentralized configuration.[327] The provisions that can be traced back to the former structure create a hierarchical construction with a clear leadership and 'chain of command'. The second approach permeates the provisions that establish a more flexible and horizontal structure between the actors. Those two structures are closely intertwined: "*(a)lthough planning occurs at a local level, this is overseen by central government; all responders are accountable to ministers for their emergency planning activities, and must take account of central government guidance in their planning [...] Central government will also become involved where an incident escalates."*[328] Authority is vested in a single body that provides a strong lead during the contingency: the command structure is linear, which can be important during emergencies. The CCA's provisions relating to cooperation and information exchange on the one hand and the respect for the autonomy of decentralized administration on the other, show the utility and importance of integrating the command and control system set up by the Act with a decentralized organizational structure. The latter adapts better to the nature of information in the ICT society: data is intangible and can be communicated in real time by and to a multiplicity of different subjects. It seems natural, therefore, in case of an emergency, where communication and coordination are of the utmost importance, resorting to a decentralized structure, as the CCA appears to do.

Regulation of Repression

Computer Misuse Act 1990

The UK's legislation appears to be already partly equipped to tackle the offences identified in the Directive 2013/40/EU on attacks against information systems. The Computer Misuse Act, in particular, can be used to address most of the offences foreseen by the Directive 2013/40/EU. A cyber attack targeting an electricity-provisioning CNI would arguably be a civil contingency, to be prevented if possible, and to be managed when – or if – it occurs. The CMA, concerned mostly with the integrity and availability aspects of the notion of security, introduced a number of (then) new offences deriving from the misuse of a computer. Notably, the CMA does not define the notion of 'computer', which contributes to making the act technologically neutral, able to cover future

[323] See CCA, Section 26.
[324] See CCA, Sections 27 and 28.
[325] See CCA, Section 29.
[326] See CCA, Section 24.
[327] See Moosavian 2014, Ibid.
[328] See Moosavian 2014, Ibid, p. 179.

technological developments, as well.[329] The act has been of course amended over the years, but the very fact that a piece of legislation drafted before the advent of the modern Internet as we know it has not been repealed yet testifies the longevity that such a legislative technique is able to grant.

The first section of the CMA introduced the offence of unauthorized access to computer material, of which a person is guilty if:

a. he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured;
b. the access he intends to secure, or to enable to be secured, is unauthorized; and
c. he knows at the time when he causes the computer to perform the function that that is the case.

Section 1 disciplines the 'basic' hacking offence, unauthorized access, which could be meant to be unauthorized access to any kind of computerized system – from a personal computer to an ICS to a networked SCADA system. Moreover, the section covers both remote hacking and unauthorized physical access like the one that can be performed by a malicious insider, e.g. an employee unduly accessing the system.

The CMA's second section is particularly relevant in the hypothetical cyber attack targeting UK electricity provisioning CNIs. Titled "*unauthorised access with intent to commit or facilitate commission of further offences,*" section 2 sanctions that a person is guilty of an offence if s/he commits the offence of unauthorized access with the intent to commit an offence to which section 2 applies[330] or to facilitate the commission of such an offence (whether alone or with another person). Notably, a person may be guilty of an offence under section 2 of the CMA even when the facts demonstrate that the commission of the further offence is impossible.

Section 3 punishes "*Unauthorised acts with intent to impair,[331] or with recklessness as to impairing, operation of computer, etc*.," sanctioning that a person is guilty of such an offence if s/he knowingly[332] or recklessly[333] does any unauthorized act in relation to a computer with the intention:

a. to impair the operation of any computer;
b. to prevent or hinder access to any program or data held in any computer;
c. to impair the operation of any such program or the reliability of any such data;
d. to enable any of the above to be done.

Section 3 appears to use interesting language, especially after the Police and Justice Act 2006 turned the offence of unauthorized modification into unauthorized impairment, thus shifting the focus from endpoint security (e.g. computers, ICS, SCADA systems, Programmable logic

[329] Michael Highfield, '*The Computer Misuse Act 1990: Understanding and Applying the Law*' (2000) 5 Information Security Technical Report, p. 53.

[330] Which are the offences "*for which the sentence is fixed by law or for which a person who has attained the age of twenty-one years (eighteen in relation to England and Wales) and has no previous convictions may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the M1 Magistrates' Courts Act 1980)*": see CMA, section 2(4).

[331] E.g. through a DDoS attack.

[332] See CMA, section 3(2).

[333] See CMA, section 3(3).

controllers, etc.) to the whole network, whenever attacking any point of the latter has an unauthorized impairing effect towards the user's computer. More questionable appears to be the choice of criminalizing reckless (even if unintentional) impairment, which could turn out to "*muddy the interpretative waters and lead to some questionable attempts at prosecution."*[334]

Section 3A, inserted by the Police and Justice Act of 2006 (c. 48) criminalizes making, adapting, supplying or offering to supply any article, if it is intended to be used to commit (or to assist in the commission of) an offence under sections 1 or 3 as sketched above.[335] It is also an offence to do so while merely believing it likely for the article's user to commit (or to assist in the commission of) an offence under sections 1 or 3.[336] Moreover, a person is also guilty of an offence "*if he obtains any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1 or 3*[337]".

The amendments to which the CMA has been subjected over the years testify to its nature: a piece of legislation drafted following a perceived regulatory gap, whose technological neutrality – arguably a positive trait when regulating technology, if properly engineered – has been repeatedly challenged. The pre-2006 version of section 3, for instance, had to have its wording changed[338] from "modification" to "impairment" by the Police and Justice Act 2006 in order to address technological issues such as the emergence of DDoS attacks.[339] The CMA's structure and history suggests that, while technological neutrality can be a positive trait in this kind of regulation, concretely applying it in practice can be tricky. Moreover, a restrictive interpretation of the wording of the act could rule out its applicability in instances where it would be natural to apply it (e.g. DDoS attacks pre-2006 amendments), while an extensive interpretation could end up criminalizing legitimate activities.

4.3 Overarching European Legislation

In addition to the country-specific legislation, one EU directive and one proposed directive are relevant with respect to protection of vital infrastructures: Council Directive 2013/40/EU (August 2013) on attacks against information systems and Proposed Directive 2013/0027 on network and information security.

[334] Neil MacEwan, 'The Computer Misuse Act 1990: lessons from its past and predictions for its future' (2008) 12 Criminal Law Review 955. http://usir.salford.ac.uk/15815/7/MacEwan_Crim_LR.pdf, p. 5 in online version.

[335] See CMA, section 3A(1).

[336] See CMA, section 3A(2).

[337] See CMA, section 3A(3).

[338] "*There have been three attempts to introduce amendment Bills to update the CMA 1990. These attempts were a response to public and industry concern around denial-of-service attacks, lobbying by the All-Party Parliamentary Internet Group (APIG) and the UK's obligations as a signatory to the COE Convention on Cybercrime5. These Bills generally failed for lack of Parliamentary time, but legislative change was finally enforced via the Police and Justice Act 2006*": Stefan Fafinski, 'The security ramifications of the Police and Justice Act 2006' (2007) 2 Network Security, p. 9.

[339] See John Worthy and Martin Fanning, 'Denial-of-Service: Plugging the legal loopholes?' (2007) 23 Computer Law & Security Review 194.

4.3.1 Council Directive 2013/40/EU of 12 August 2013 on attacks against information systems

Directive 2013/40/EU on attacks against information systems,[340] which replaces the Council's Framework Decision 2005/222/JHA, was drafted partially in consideration of potential cyber attacks targeting national CNIs. As the Directive notes, "*There is evidence of a tendency towards increasingly dangerous and recurrent large-scale attacks conducted against information systems which can often be critical to Member States".*[341] "The objectives of this Directive are to approximate the criminal law of the Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions and to improve cooperation between competent authorities, including the police and other specialised law enforcement services of the Member States, as well as the competent specialised Union agencies and bodies, such as Eurojust, Europol and its European Cyber Crime Centre, and the European Network and Information Security Agency (ENISA)."[342] This directive inter alia ensures that all Member States have criminalized a number of general computer crimes, such as illegal access to information systems or illegal system interference.

Furthermore, it "*has become apparent from the need to increase the critical infrastructure protection capability in the Union that the measures against cyber attacks should be complemented by stringent criminal penalties reflecting the gravity of such attacks."*[343] Hence, the Directive aims to establish a minimum set of rules defining criminal offences and sanctions in the area of attacks against information systems and facilitating their prevention, as well as to improve cooperation between the relevant authorities[344]. In particular, articles 3 through 8 of the Directive identify a number of offences (namely: Illegal access to information systems, illegal system interference, illegal data interference, illegal interception, making available tools designed or adapted primarily to commit the aforementioned offences and inciting, aiding and abetting the commission of one of those aforementioned offences) that are to be implemented by member states in order to ensure an adequate level of protection and security of information systems.

Two other articles of the Directive are also relevant in addressing the possibility of a cyberattack targeting a CNI. Cooperation and information exchange between member states is fostered by the Directive's Article 13, "*Exchange of information*", according to which "*Member States shall ensure that they have an operational national point of contact and that they make use of the existing network of operational points of contact available 24 hours a day and seven days a week. Member States shall also ensure that they have procedures in place so that for urgent requests for assistance, the competent authority can indicate, within eight hours of receipt, at least whether the request will be answered, and the form and estimated time of such an answer*". Article

[340] Council Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L218/8.

[341] Directive 2013/40/EU, Recital 5.

[342] Recital 1 of the directive.

[343] Directive 2013/40/EU, Recital 4.

[344] Directive 2013/40/EU, Art. 1.

14, titled “*Monitoring and statistics*”, mandates that Member States must have a system for recording, producing and providing statistical data regarding the offences foreseen in the Directive.

4.3.2 Proposed Directive 2013/0027 on network and information security[345]

The main relevant provisions of the NIS Directive, which is not yet in force, are the following. ‘Responsibilities in ensuring NIS lie to a great extent on public administrations and market operators. A culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced should be promoted and developed through appropriate regulatory requirements and voluntary industry practices.’[346] ‘Member States shall ensure that public administrations and market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.’[347] ‘To ensure convergent implementation of Article 14(1), Member States shall encourage the use of standards and/or specifications relevant to networks and information security.’[348][349]

The concept ‘network operator’ in this directive encompasses operators of critical infrastructures that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health (art.3(8)). The proposed Directive creates a cooperation mechanism between Member States in order to ensure a coordinated and efficient handling of and response to risks and incidents affecting network and information systems. The directive requires all Member States to have a national "competent authority" on the security of network and information systems (art.6(1)). The competent authority receives notifications of incidents from public administrations and market operators and is granted implementation and enforcement powers, viz. to: investigate noncompliance by market operators and public administrations, to require them to provide information and to undergo a security audit, and to issue binding instructions (art. 6(4) & 15). Each Member State must set up a CERT responsible for handling incidents and risks according to a well-defined process (art.7(1)).

[345] Proposal for a Council Directive 2013/0027 concerning measures to ensure a high common level of network and information security across the Union [2013] COM (2013) 48 final: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0048&from=EN

[346] Recital 22.

[347] Art. 14(1).

[348] Art. 16(1).

[349] A relevant standard: ISO/IEC TR 27019:2013 Information technology – security techniques – information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry, see Annex 1.

4.4 Conclusion

This chapter examines the governance of cybersecurity with regard to vital infrastructures. It describes relevant actors and regulatory measures for the energy sector to gain better understanding of how vital infrastructures are protected in the selected countries. Although we only focus on this aspect of vital infrastructures, the quick scan revealed that part of the problem across the board lies in the broad definition of what constitutes a vital infrastructure. Canada, for instance, lists ten different infrastructures that fall in the category critical (or vital), and Germany has a similarly broad approach to defining critical infrastructures. The combination of numerous policy documents containing generally vague recommendations, with a large, and growing, number of actors that are somehow related to the governance of vital infrastructures, make the field hard to oversee – not only for research purposes, but also, critically, for governance purposes.

This leads to a second problem that the countries share – they all struggle (to a greater or lesser degree) with how to coordinate across different types of actors and resolve tensions that arise with respect to sharing responsibility between public and private parties. This was especially evident in Canada, where investments in cybersecurity measures are borne by operators. The benefit that private investment in cybersecurity brings is to a large extent a social benefit; in other words, an externality for the operator. Whereas, in Estonia, coordination is achieved through the preventive measures that spearhead the regulation of CI and CII protection, in other countries this was more difficult to achieve. The case of Germany, especially, shows that there are still few obligations for actors regarding prevention, reporting and other action for critical infrastructure operators, yet attempts to impose stricter measures for responsible parties (including emphasizing the BSI's central role in cybersecurity issues and expanding the Federal Criminal Police Office's authority to investigate computer-related crime) met serious resistance from industry. CNI protection in the UK is a joint effort between the relevant national and corporate stakeholders; the public and the private sectors appear to be interdependent and work together in order to ensure the safety of the CNI. After liberalization of the Dutch energy market, new market players emerged, leading to an unbundling of functions, with oversight being distributed over multiple institutions. The Dutch network is also more intensely connected to foreign networks, which has led to a greater need for cross-border coordination.

This chapter highlights not only the importance of consideration for economic factors, but also the need for coordination in the governance of cybersecurity: the choice of new measures to take touches upon the general interest and therefore legitimises certain government involvement in stipulating the responsibilities of private actors. In the cases discussed here, two types of institutionalization can be discerned: institutionalization in the energy domain and institutionalization in the cybersecurity domain. This seems to play more strongly in some areas (incidents) than others (repression), whereby there may not be enough awareness of cyber security threats. We also see in these cases how the notion of governance-as-process takes shape in practice; public and private actors search together for the proper constellation of measures, especially as markets change and new actors join. The role of the state with regard to governance of many of these interactions takes on the form of providing a framework of rules within the boundaries of which private actors are allowed to act, with some (Estonia) being more strict than others (Germany). Public actors in the UK interact closely with the private sector, providing guidance, best practices and collaboration, rather than regulation. Generally speaking, in the prevention stage, more parties need to make calamity plans that are well-attuned to one another. In the incident stage, more complex information streams are needed, to inform both the field and government institutions (both internally and abroad). Cybersecurity-specific institutionalization may help raise major players' awareness of potential security risks, but should be approached carefully, as they could also potentially create too much red tape.

5. Case 3: Protection of Identity Infrastructures

5.1 Introduction

In the offline world, we are familiar with the idea that identities are provided by the state. At birth our identity is established through registration at the municipal registry. The state acknowledges the newborn by registering its first name(s) in association with the surnames of the parents. The state also issues identifiers such as an identification or social security number, not only at birth, but also later in life. Individuals in many countries are obliged to carry state-provided identity documents to be able to identify and authenticate their identity claims. State issued identity documents are powerful because they are accepted throughout society, both in the public and private sector as proper identity tokens.

But these are not the only identification documents that we acquire over our lifetime. More and more, companies and institutions use their own internal identification methods. Examples of such non-state provided identifiers include: banking cards to withdraw money from ones account, key cards to enter corporate buildings, student cards to prove eligibility to complete exams and the combination of user account names + passwords for online transactions. In some cases these “internal identification methods” are linked to use in other contexts: for example, a student-card can be used to get a discount at the local bookstore and bank cards, credit cards, library passes, frequent flyer passes, loyalty cards, etc, represent partial identities in everyday life. The trustworthiness of these identities may vary significantly.

The identity management landscape revolves around the core processes in the IAA model: identification, authentication and authorisation. Identity management can be seen as access control to resources. In the identification process, a person requesting access to resources will present an identity claim: I am root. This claim may be true or false. In order to asses the validity of a claim, authentication will take place: is this really root? This can be done in different ways. There are four general methods for authenticating claims:

1. What you know – e.g., the password or phrase;
2. What you do -- e.g., how one signs one's name or speaks;
3. What you are -- e.g., one's face or other biometric attributes such as fingerprints;
4. What you have -- e.g., a token such as a key or a certificate such as a driver's license.

The certainty the recipient requires to have regarding the validity of the claim determines what can be used to authenticate the claim. In everyday life, we often use auditory (voice) or visual (looks) recognition to authenticate the people we know. If more certainty is required, (state issued) identity documents may be necessary. The final step in obtaining access to resources is authorisation: is this person supposed to be able to access the resource. An individual X who is successfully authenticated as being X is not necessarily authorised to access a given area. In other words, authorisation ascertains which resources a person may use given that he has proven (authentication) to be who he claims to be (identification). It should be noted, however, that authorisation does not necessarily have to follow identification: in various contexts, it may be sufficient to establish whether someone is authorised to something (e.g., buy alcohol, enter a building) without having to know the identity of the person.

The identity management landscape consists of a number of parties:[350]

- Claimant: The claimant (citizen or consumer) is the entity that wants to use a certain service or access certain resources. The claimant may need to identify and/or authenticate him/herself for this purpose.
- Relying party: The relying party is the entity that relies on the claim that the “claimant” is who s/he claims to be. Relying parties may be public entities, such as local governments or large national public services, in which case they are also called Government Service Providers (or GovSP). Private entities can also be relying parties; these are also known as Commercial Service Providers (ComSP).
- Identity provider: The identity provider is the entity that can provide a claimant an identifier. The identity provider is a Registration Authority responsible for verifying the (real world) identity of the subscriber typically through the presentation of paper credentials and by records in databases. The RA, in turn, vouches for the identity of the subscriber to a CSP.
- Attribute provider: An attribute provider can provide the claimant or a relying party (certified) attributes of the claimant. Attribute providers can be public entities (GovAP) or commercial entities (ComAP). In the Dutch public sector the GBA (Municipal Registry) is an attribute provider. In the private sector, for instance, banks could be attribute providers for bank account numbers.
- Certificate/Credentials service provider: A certificate service provider (CSP) can provide other parties in the architecture with certificates that can be used for authentication, such as server certificates to GovSPs and ComSPs, authentication certificates and signature certificates to claimants. CSPs may also provide validation services for certificates by means of OCSP (Online Certificate Status Protocol) services and Certificate Revocation Lists.
- Authentication service provider: An ASP is a party that can authenticate a claimant as being who she says to be.

The IAA model introduces the notion of a process in identity management. Identification, authentication and authorization are part of a broader set of processes relating to the issuing of identities and the subsequent use of these identities in daily life, governance of which must be coordinated across the aforementioned parties.

[350] We follow the IDABC terminology here (IDABC, 2007, p. 16-18).

This chapter examines how the identity infrastructure for citizen-government relations is organized in the selected countries.

1) *Who and how* - Which actors are responsible for taking which actions? What is the organisational and institutional arrangement? What is the remit of actors to act?

2) *What and why* - What does the content of the regulation aim to achieve? What is the definition of identity infrastructures?

3) W*here* - In which places is the challenge being addressed in practice, e.g. sectors, (self)-regulatory arrangements, illustrative cases?

These aspects, taken together, address the following question: *how is secure authentication of citizens in the context of e-government, in particular electronic service delivery, organized?* The cases are discussed in the following order: Canada, Estonia, Germany, the Netherlands and the UK.

5.2 Case Study Countries

Each case begins with a short introduction, followed by an outline of relevant actors and overview of applicable legislation. As in Chapter 4, in examining the regulatory framework for each case, we distinguish between regulation of prevention, regulation of incident management and regulation of repression (although there is occasional overlap).

5.2.1 Canada

According to a study by McMaster University[351] 1.7 million Canadians were victims of identity theft in 2008.[352] In 2014, detailed tax information about well-known Canadians was leaked from the Canada Revenue Agency to CBC News.[353] As is mentioned in Chapter 4, the Royal Canadian Mounted Police published a document on cybercrime that describes Canada's digital landscape and focuses on aspects of the cybercrime environment that affect Canada's public organizations, businesses and citizens in real and harmful ways.[354] It covers a broad range of cyber incidents. Cyber incidents concerning identity infrastructure are also specifically mentioned by the Digital Identification and Authentication Council of Canada (DIACC). These include the 'Heartbleed vulnerability', the breaches at Target and Home Depot and breaches at government organizations such as Canada Revenue Agency and the National Research Council of Canada. The Target and Home Depot breaches concern hackers stealing large collections of card numbers and other pieces of customer data from these large retailers.[355] Aside from these two documents, policy documents relevant to the governance of identity infrastructures include the Cyber Security Strategy of 2010

[351] Susan Sproule and Norm Archer, 'Measuring Identity Theft in Canada: 2008 Consumer Survey' (McMaster University Working Paper, 2008). Available at: http://merc.mcmaster.ca/measuring-identity-theft-canada-2008-consumer-survey/

[352] National Cybersecurity Strategy 2010, p.4.

[353] See http://www.cbc.ca/news/politics/canada-revenue-agency-privacy-breach-leaks-prominent-canadians-tax-details-1.2849336

[354] http://www.rcmp-grc.gc.ca/pubs/cc-report-rapport-cc-eng.htm

[355] See http://www.reuters.com/article/2014/09/09/us-usa-home-depot-databreach-idUSKBN0H327E20140909

(NCS 2010)[356] and 'Action Plan 2010-2015 for Canada's Cyber Security Strategy' (APCS 2010)[357] mentioned in Chapter 4, as well as the 'Policy on Government Security' of 2009, administered by the Treasury Board Secretariat.[358]

In Canada, the jurisdiction of identity is 'a responsibility separated between the federal, provincial and territorial governments. Digital identity is defined by the Government of Canada as: 'an identity developed in the online environment that can be accessed, used, stored, transferred or processed by means of electronic of computer devices or systems'.[359] The traditional approach with respect to identity has been to work independently within each jurisdiction.'[360] There are currently at least six independent initiatives towards electronic identity instruments, including:

- The Canadian e-passport: a traditional paper passport with an added secure chip.[361]
- BC Services Card: 'a provincially issued smart services card'[362] introduced in 2013 to facilitate access to provincial government services for residents of British Columbia.
- The Electronic Identity Verification (EIV) initiated by the Ministry of Justice of British Columbia[363] is a tool used to verify the identity of an individual and ensure the accuracy of personal information contained in the criminal record check form.
- SecureKey Sign-In Partner Login for Government of Canada: this program minimizes the need for users to remember multiple passwords by allowing them to sign in using a username and password from another reliable system (organizations that have partnered with SecureKey for this purpose). The service acts as an information filter to ensure that the government services do not know which sign-in partner is used and that no sign-in partner knows which government service is being accessed.[364] SecureKey Concierge allows citizens to use their bank credentials as identification on government services websites.[365]
- ONe-key: a unique electronic credential (double-blind solution) that allows citizens to communicate securely with online Government services.[366]

[356] Available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/canadaNCSS.pdf

[357] Available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf

[358] Additional documents and initiatives about the identity infrastructure include: Canada Health Infoway, 'Federated Identity Management in Health Care White Paper' (2014); Joint Councils of Federal, Provincial and Territorial Deputy Ministers' Table on Service Delivery Collaboration, 'Pan Canadian Identity Validation Standard' (2014). It standardizes identity validation requests and responses between federal, provincial, territorial and municipal government organizations (evolution of the National Routing System). The Identity Management Steering Committee, 'Trusting Identities: Pan-Canadian Approach to Enabling better Services for Canadians' (2011). Joint Councils of Federal, Provincial and Territorial Governments/Identity Management Steering Committee, 'Pan Canadian Assurance Model' (2010). Inter-Jurisdictional Identity Management and Authentication Task Force, 'Pan-Canadian Strategy for Identity Management and Authentication' (2007).

[359] Industry Canada, 'Digital Policy Branch', available at: https://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00585.html

[360] Digital Identification and Authentication Council of Canada, 'Building Canada's Digital Identity Future' (May 2015), p.5.

[361] http://www.cic.gc.ca/english/department/media/multimedia/video/e-passport/e-passport.asp

[362] http://www2.gov.bc.ca/gov/topic.page?id=87EEAD6D19974459950AA7FF7F60AD54

[363] http://www.pssg.gov.bc.ca/criminal-records-review/eiv/index.htm

[364] DIACC, p. 12.

[365] http://securekeyconcierge.com/

[366] DIACC, p. 49.

- Ontario Go-Secure: enables secure access to government applications for internal employees, extranet users and agents of the government.[367]

From the perspective that, ‘Digital identity requires a pan-Canadian approach that is interoperable with different systems be they federal, provincial, territorial or private sector,’[368] a Joint Council of Federal, Provincial and Territorial Governments is now working on a ‘Pan-Canadian Identity Trust Framework’. The DIACC proposed the ‘Federated Authentication and Brokered Authorization Model’ (2014-2015) as an approach for Canada’s digital identification ecosystem[369] that involves four main actors (the individual, the relying party, the authoritative party and the core digital identification and authentication platform service). The model is built on seven universal requirements of a digital ecosystem and four specifically Canadian requirements.

Universal requirements:

1. Robust, secure, scalable
2. Privacy protecting/privacy enhancing
3. Inclusive and transparent
4. Meets broad stakeholder needs
5. Data minimization
6. Knowledge and consent
7. Convenient

Canadian requirements:

1. Built on open, standards-based protocols
2. Interoperable with international standards
3. Cost effective and open to competitive market forces
4. Able to be independently assessed, audited and subject to enforcement

However, this Federated Authentication and Brokered Authorization Model is currently just a proposal; it does not reflect the current situation in Canada.

Relevant Actors

The following actors are relevant to the governance of identity infrastructures in Canada[370]:

- Public Safety Canada provides central coordination to address risks within the Government and across Canada. Public Safety Canada also leads public awareness and outreach activities to inform Canadians of the potential risks they face and the actions they can take to protect themselves and their families in cyberspace.
    - Canadian Cyber Incident Response Centre monitors and provides mitigation advice on cyber threats and coordinates the national response to any cybersecurity incident. It falls under the responsibility of Public Safety Canada.

[367] DIACC, p. 49.

[368] Digital Identification and Authentication Council of Canada, ‘Building Canada’s Digital Identity Future’ (May 2015), p.5.

[369] DIACC, p. 14 and 19-24.

[370] Reference information for information on those actors already named in Chapter 4 is located in that chapter.

- Foreign Affairs and International Trade Canada advises on the international dimension of cybersecurity and work to develop a cybersecurity foreign policy that will help strengthen coherence in the Government's engagement abroad on cybersecurity.
- Treasury Board Secretariat administers the Policy on Government Security, which sets out safeguards to assure the delivery of Government services to Canadians.
- Communications Security Establishment Canada detects and discovers threats, provides foreign intelligence and cyber security services, and responds to cyber threats and attacks against Government networks and information technology systems.
- Canadian Security Intelligence Service analyses and investigates domestic and international threats to the security of Canada.
- The Royal Canadian Mounted Police investigates, as per the Royal Canadian Mounted Police Act, suspected domestic and international criminal acts against Canadian networks and the critical information infrastructure.
- The Digital Identification and Authentication Council of Canada (DIACC), a non-profit coalition of public and private sector leaders formed in 2012, is identifying the best avenue to developing a robust, secure, scalable and privacy-enhancing digital identification and authentication ecosystem that would suit the needs of all stakeholders. DIACC collaborates actively with two pan-Canadian Councils, the Public Sector Service Delivery Council (PSSDC)[371] and Public Sector Chief Information Officer Council (PSCIOC).[372] Reporting to these two councils is the Identity Management Sub Committee (IMSC).[373]
- Office of the Privacy Commissioner of Canada. The Privacy Commissioner of Canada is an Officer of Parliament who reports directly to the House of Commons and the Senate and is an advocate for the privacy rights of Canadians. [374]
- Provinces and territories provide a range of essential services for which delivery is dependent on the safe and secure operation of their cyber systems. For example, they hold sensitive personal information in their electronic databases, including health records, marriage and driver licenses, and provincial tax return information.[375]
- Critical infrastructure owners and operators bear the primary responsibility for protecting their assets and services.
- Individual Canadians have a responsibility to be alert to threats of identity theft or fraud. The RCMP provides information to the public.[376]

[371] http://www.iccs-isac.org/en/councils/pssdc/
[372] http://www.iccs-isac.org/en/councils/pscioc/
[373] http://www.iccs-isac.org/councils/joint-councils/identity-management-sub-committee/?lang=en
[374] https://www.priv.gc.ca/au-ans/index_e.asp
[375] NCS 2010, p.11.
[376] http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-eng.htm

Regulatory Framework

In the 'National Strategy for Critical Infrastructure,' the national government and the provinces distinguish ten critical infrastructures. Identity management is not identified as a separate critical infrastructure but is caught in the broader category of 'Information and Communication Technology'. New regulatory initiatives relevant for the security of e-identities address a mix of identity specific and broader issues.

Regulation of Prevention

Standard on Identity and Credential Assurance (2013)[377]

This standard is administered by the Treasury Board Secretariat. The objective of the standard is to 'ensure that identity risk is managed consistently and collaboratively within the Government of Canada and with other jurisdictions and industry sectors.' The standard gives rules for determining the identity and credential assurance levels required for the application at hand, selecting suitable controls and ensuring that the minimum requirements for establishing the selected identity assurance level are met. It further contains rules about federating identity, monitoring compliance (within the own organization), addressing gaps in performance and reporting. The Treasury Board of Canada Secretariat has the task of government–wide monitoring and reporting.

Further regulation

Other guidelines include: 'Guidelines for Identification and Authentication' (2006) by the Office of the Privacy Commissioner,[378] Industry Canada's 'Canada's Principles for Electronic Authentication' (2004),[379] and the Treasury Board Secretariat's 'Directive on Identity Management' (2009).[380]

The Guidelines for Identification and Authentication are applicable in the relation between individuals and organizations. The guidelines state principle-like guidelines, such as 'only authenticate when necessary', and 'level of authentication commensurate with the risk'. Other guidelines are more practical, such as : responding to changing threats, regularly monitor threats, employee training, responsibility of individuals, changing authentication information (such as passwords), individual choice in identification and authentication options, easy to remember, difficult to guess (passwords), authentication should not be based on personal identity facts, reliance on verifiable tokens, safeguards for integrity of authentication processes, audit logs and responsibility for outsourcing.

Canada's Principles for Electronic Authentication (CPEA) 'were developed by the Authentication Principles Working Group, convened by Industry Canada and with broad representation from industry, professional associations, consumer groups and various levels of government.'[381] 'The CPEA identify the functions and responsibilities of participants in authentication processes and provide a framework to assess and manage the risks that accompany

[377] http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776

[378] https://www.priv.gc.ca/information/guide/auth_061013_e.asp

[379] https://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/h_gv00240.html

[380] http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577

[381] CPEA, p.3.

these responsibilities. The Principles also identify security, privacy, disclosure and complaint handling matters that need to be taken into account at each stage of the design, development, implementation and assessment of an authentication process.'[382]

The Directive on Identity Management (DIM) is applicable to governmental departments. Its objective is 'to ensure effective identity management practices by outlining requirements to support departments in the establishment, use and validation of identity.'[383]

Regulation of Incident Management

Privacy Act

'Federal institutions subject to the Privacy Act are required to notify the Office of the Privacy Commissioner of Canada (OPC) and the Treasury Board of Canada Secretariat of all material privacy breaches and of the mitigation measures being implemented, if the breach involves sensitive personal information and could reasonably be expected to cause serious injury to the individual.'[384] Reports of data breaches involving personal data are an important source of information about cyber security incidents.

Amendments to the Personal Information Protection and Electronic Documents Act

The government has introduced a bill in parliament that strengthens the obligations concerning notification with regard to security breaches. It concerns bill S-4, amending the Personal Information Protection and Electronic Documents Act (PIPEDA). S-4 adds three new sections to PIPEDA: 10.1, 10.2 and 10.3, dealing with 'Breaches of Security Safeguards'. An organization that has experienced a breach of security safeguards involving personal information under its control will be required to provide notification in three circumstances:

- to the Privacy Commissioner, 'if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual';
- to the individuals whose personal information is involved, 'if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual'; and
- to other organizations or government institutions, 'if the notifying organization believes that the other organization or the government institution may be able to reduce the risk of harm that could result from the data breach or mitigate that harm'.

To section 2(1) PIPEDA a definition of a 'breach of security safeguards' is added. It defines it as 'the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 or from a failure to establish those safeguards.''[385]

[382] CPEA, p.4

[383] Art. 5.1 DIM.

[384] https://www.priv.gc.ca/resource/pb-avp/pb-pa_e.asp See also art. 6.1.2 Directive on Privacy Practices.

[385] See https://www.priv.gc.ca/parl/2014/parl_sub_140604_sen_e.asp

Regulation of Repression

In 2009, the criminal code was adapted to account for identity theft and identity fraud. In section 402.1 an elaborate definition of identity information is given:

> 402.1 For the purposes of sections 402.2 and 403, “identity information” means any information — including biological or physiological information — of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual, including a fingerprint, voice print, retina image, iris image, DNA profile, name, address, date of birth, written signature, electronic signature, digital signature, user name, credit card number, debit card number, financial institution account number, passport number, Social Insurance Number, health insurance number, driver’s licence number or password.

Section 402.2 about trafficking in identity information criminalises behaviour that in itself is not damaging, but can be seen as a preparation for such behaviour.

> 402.2 (1) Everyone commits an offence who knowingly obtains or possesses another person’s identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.
> (2) Everyone commits an offence who transmits, makes available, distributes, sells or offers for sale another person’s identity information, or has it in their possession for any of those purposes, knowing that or being reckless as to whether the information will be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.[386]

The offences criminalised in section 402(2) can be punished with imprisonment up to 5 years.

The actual identity fraud is criminalised in section 403:

> 403. (1) Everyone commits an offence who fraudulently personates another person, living or dead,
> (a) with intent to gain advantage for themselves or another person;
> (b) with intent to obtain any property or an interest in any property;
> (c) with intent to cause disadvantage to the person being personated or another person; or
> (d) with intent to avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice.
> (2) For the purposes of subsection (1), personating a person includes pretending to be the person or using the person’s identity information — whether by itself or in combination with identity information pertaining to any person — as if it pertains to the person using it.

Such criminalization of these acts shows that identity theft and misuse is taken seriously in Canada.

[386] Art. 402.2(3) For the purposes of subsections (1) and (2), an indictable offence referred to in either of those subsections includes an offence under any of the following sections: (a) section 57 (forgery of or uttering forged passport); (b) section 58 (fraudulent use of certificate of citizenship); (c) section 130 (personating peace officer); (d) section 131 (perjury); (e) section 342 (theft, forgery, etc., of credit card);
(f) section 362 (false pretence or false statement); (g) section 366 (forgery); (h) section 368 (use, trafficking or possession of forged document); (i) section 380 (fraud); and (j) section 403 (identity fraud).

5.2.2 Estonia

In Estonia, the concept of e-government was created already at the end of 1990s[387] and is based on the secure data exchange layer X-Road[388] and digital IDs issued by the state.[389] During the validation interview for this research, the head of the Department of Information Society Services Development at the Ministry of Economic Affairs and Communications (MEAC) pointed out three key decisions that could be described as *key enablers* of the development of government e-services (e.g. e-tax board, e-voting, e-medicine etc.), the success and widespread use of the digital-ID and m-ID and the launch of an e-resident's[390] digital ID in Estonia:[391]

1. Issuing personal identification codes to every citizen. As a result, every citizen has a unique number that can be processed by information systems. Such a code is not deemed as sensitive personal data by the Estonian Data Protection Inspectorate.[392]
2. Promoting digital procedures as equal to physical procedures, as well as the state's obligation to communicate and offer both online and offline services. This enabled a swift move to a 'paperless' bureaucracy (of course, not all paper is gone, but the idea that digital procedures and signatures are as real as paper is now deeply rooted in the minds of Estonians).
3. Implementing the "ask data once only" principle which means that the state asks the data subjects' (including businesses) data only once and shares it with different state and government institutions, instead of every institution repeatedly requesting the same data.

These three decisions, together with the X-Road, enabled the creation of the current Estonian ID architecture. The different services and channels of communication (see Case Example in the Text Box) are discussed below.

Relevant Actors

In Estonia, the following actors are relevant to the governance of identity infrastructures:

[387] In 1998, the Parliament of Estonia (*Riigikogu*) adopted a document named the "Founding Principles of the Estonian Information Policy" (*Eesti infopoliitika põhialused*) which set out the principles of operation of the public sector.

[388] The X-road is the backbone of the government's e-services – it is a data exchange layer linking different databases and state's information systems. The X-Road enables securely exchanging data as well as to ensure people's access to the data maintained and processed in state databases. Public and private sector enterprises and institutions can connect their information system with the X-Road. This enables them to use X-Road services in their own electronic environment or offer their e-services via the X-Road. Joining the X-Road enables institutions to save resources, since the data exchange layer already exists. See <https://www.ria.ee/x-road/> accessed 31 May 2015.

[389] R Annus 'E-residentsus' (2014) 10 Juridica, p. 740 <http://juridica.ee/get_doc.php?id=2160> accessed 3 June 2015.

[390] As of 1 December 2014, Estonia has opened its e-services to foreigners who wish to conduct business in Estonia or otherwise have a link to Estonia. An 'e-resident' may apply for a digital identity card (digi-ID) that enables digitally signing documents and using public and private IT solutions that require the highest level of authentication. The digi-ID does not enable authentication in the offline world.

[391] Interview with Janek Rozov (Tallinn, 8 May 2015).

[392] Guidelines on the use personal identification code (in Estonian) by the Estonian Data Protection Inspectorate <http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikukoodi%20kasutamise%20juhend_0.pdf> accessed 3 June 2015. However, some restrictions still apply, e.g. the name and the personal identification code should not be used together if possible.

- The state undertakes to assure the existence and functioning of a public key infrastructure (PKI)[393] by: (1) providing and ensuring functioning base software for the ID-card; (2) setting out the rules that determine the quality and trust requirements of the PKI services; and (3) handling the issuance of the means for secure electronic authentication and signing. The first point is an obligation of a sub-unit of MEAC, the Information Systems Authority (ISA). The third falls under the authority of the Police and Border Guard (PBG).
- Certification Centre (CC)[394] is a private party that ensures the reliability and integrity of the electronic infrastructure of the ID-card (further discussed below).
- ISA is a sub-unit of MEAC that is responsible for ensuring ID-card software functioning (as mentioned in point one under the state's responsibility for PKI).

Case Example: The Digital ID Card and Communication between Citizens and the State

The compulsory ID-card is a key for communicating with the state for both citizens and companies. Every ID-card owner has a personal e-mail address, issued by the Republic of Estonia. This address is intended to be an official channel of communication between the state and the person. The state can use this address to send a given individual official notices and personal information related to the person or situation. Other persons can also send messages to this address.

For citizens, the website www.eesti.ee is the starting point of using the government's e-services. Eesti.ee comprises more than 300 e-services and enables filing different (pre-filled) applications, making inquiries in different databases, voting in the local or parliamentary elections, entering the e-Tax Board, entering the e-Land Register and entering the patient's electronic health record portal digilugu.ee. Entering eesti.ee requires the codes of the ID-card and relevant software. Eesti.ee is not a large database itself; rather, it consists of distributed information systems under different Ministries and institutions. Distributed architecture is what makes it safe. Of course, eesti.ee enables changing personal data as well, e.g. change of place of residence and contact details.

For businesses, the ID-card enables entering the e-Business Register, where it is possible to establish a company online without the need to go to a notary public or any other government office. The e-Business Register also allows entrepreneurs to submit electronic applications, documents and annual reports to the Commercial Register.

Because the ID-card is considered to be the safest manner of authentication, it is also used by banks to enable customers to make secure payments and log into their web platforms with the digital-ID or the mobile-ID. Some banks enable transferring larger amounts of money when signing in with a digital-ID or a mobile-ID, as the state ID infrastructures provide higher security standards.

As a counter-measure, eesti.ee also enables a citizen to see which institutions (e.g. Police or a bank) have made queries of his/her data. Thereby, the citizen – as a data subject – is given some control over his or her data in the state's information systems.

The overall use of e-government services by individuals was 51% in 2014, whereas the use of e-services by businesses is more commonplace (95% in 2013).

[393] See <https://www.ria.ee/en/?id=27307> accessed 3 June 2015.

[394] Certification Centre is currently the only certification authority in Estonia providing certificates for authentication and digital signing to the ID-card, digital-ID and mobile-ID. See <https://sk.ee/en/about/> accessed 4 June 2015.

Regulatory Framework

The main sources of law are the Identity Documents Act and the Digital Signatures Act. As indicated below, together, these underlie the ID-card that enables both offline and online identification.

Regulation of Prevention

The main sources of law in this regard are the Identity Documents Act (IDA) and the Digital Signatures Act (DSA). According to IDA, the ID-card is a compulsory identity document of any Estonian citizen or citizen of the European Union residing permanently in Estonia on the basis of a valid right of residence.[395] Issued since 2002, the ID-card enables both online and offline citizen identification.[396] The ID-card is also a travel document within the European Union.[397] Together with the physical ID-card, the owner of the ID-card receives certificates that enable identifying the owner of the ID-card in the online environment.[398] The ID-card has two certificates: one for identifying the person and one for the digital signatures.[399] In addition to the ID-card, authentication is possible via mobile-ID. The function is the same – two sets of certificates that enable identification of a person and the grant of digital signatures.[400]

The DSA provides that a digital signature has the same legal consequences as a hand-written signature.[401] The DSA is also the basic document for CC, as it contains provisions regarding the provision of certification services and time stamp services.[402] In order to prevent abuse of a lost or stolen ID-card, the DAS obliges the CC to accept applications for the suspension of certificates twenty-four hours a day.[403]

Regulation of Incident Management

The Statute of ISA stipulates that ISA is the responsible body for handling cyber-incidents in Estonian networks.[404] Internally, the task is delegated to the sub-unit CERT.[405] The RFC 2350 Description of CERT-EE stipulates that CERT-EE will provide assistance or advice with respect to the following aspects of incident management[406]:

- Incident triage: investigating whether an incident indeed occurred and determining the extent of the incident;

[395] See section 19 of the Identity Documents Act.
[396] See section 19^1 of the Identity Documents Act.
[397] See <http://www.id.ee/?lang=en&id=34395> accessed 27 July 2015.
[398] When receiving the ID-card, the person receives an envelope which includes three codes: PIN1 (identification; 4 digits), PIN2 (digital signature; 5 digits) and PUK (8 digits). The PIN codes can be changed in the ID-card utility program (downloadable software that enables identification, encryption and signing documents digitally). If a person loses or forgets the PIN codes, new codes may be obtained from a service point of Police and Border Guard Board (for free) or a bank branch (for a fee).
[399] See <http://www.id.ee/index.php?id=30228>. According to the Digital Signatures Act, a "digital signature" is a data unit, created using a system of technical and organisational means, which is used by a signatory to indicate his or her link to a document.
[400] See section 19^1 of the Identity Documents Act.
[401] See section 3 of the Digital Signatures Act.
[402] Subsection 3(1) of the Digital Signatures Act.
[403] Subsection 22(4) of the Digital Signatures Act.
[404] Subsection 8(3) of the Statute of ISA.
[405] Subsection 13(1) of the Statute of ISA.
[406] See <https://www.ria.ee/rfc-2350/> accessed 2 August 2015.

- Incident coordination: determining and contacting the involved organizations, facilitating contact with other parties (incl. law enforcement) asking for and/or composing reports and, when necessary, communication with the media;
- Incident resolution: advising the involved organizations on appropriate measures, following up the incident solution process and collecting evidence and interpreting data.

Regulation of Repression

The Penal Code has criminalised the following acts regarding ID-cards: falsification, obtaining, using or granting permission to use a falsified ID-card and fraudulent use of an ID-card (see, respectively, sections 347, 348 and 349 of the Penal Code).

5.2.3 Germany

Secure and user friendly identity management is one of the goals of the German ICT Strategy[407] and of the German e-Government initiative.[408] In Germany, the identity management strategy is based on (a) the switch from a paper-based identity card to an electronic identity card enabling citizens to authenticate themselves in e-government communication; (b) citizens portals certified to providing secure Email and identity verification services and (c) SAFE – the technical framework enabling the safe usage of digital identities across administrative borders.[409]

This section focuses on the deployment of electronic identity cards in Germany and the eID infrastructure put in place to enable the electronic authentication function of the ID cards. Public authentication schemes based on identity cards were in place long before internet; governments and businesses trust government issued cards for the purposes of reliable authentication of citizens.[410] These conventional identification processes are generally not applicable on the Internet, even though online processes and transactions often require that one knows who her communication partners are.[411] In Germany, the trust in government issued cards has been extended to electronic identity cards with regard to fulfilling the same purpose in electronic communications. The new identity card (neuer Personalausweis) was advertised as the 'most important card,'[412] when it came into effect on 1 November 2010. This electronic and multi-functional card serves as a travel document and proof of identity both in personal contact and electronically. For the latter purpose, the card is equipped with additional functions: (1) the electronic ID (eID) containing an identity record that authorized services can access with the permission of the card holder; (2) the ePass function reserved for government use; and (3) the optional qualified electronic signature function. Individuals can utilize these functions to positively

[407] Bundesministerium für Wirtschaft und Technologie (2010), *ICT Strategy of the German Federal Government: Digital Germany 2015,* Munich: BMWi, p. 18.

[408] See: http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/E-Government/E-Government-Initiative/e-government-initiative_node.html

[409] OECD (2011), *National Strategies and Policies for Digital Identity Management in OECD Countries,* OECD Digital Economy Papers, No. 177, OECD Publishing, p. 48.

[410] A Poller, U Waldmann, S Vowé, and S Türpe, '*Electronic Identity Cards for User Authentication – Promise and Practice*' (2012), p. 47.

[411] G Hornung and A Roßnagel, 'A*n ID card for the Internet – The new German ID card with "electronic proof of identity"*' (2010), p. 153.

[412] Poller et al. 2012, p. 47.

identify themselves online and issue binding declarations of will electronically in eGovernment and eBusiness services.[413] Function (1) eID is the focus of this section.

The introduction of the new identity card and related infrastructure has been justified by a need for a trustworthy and efficient identity management. This need is to be realized by a combination of a sovereign identity document with eID functionality for eBusiness and eGovernment that aims to provide users with a secure identity in the electronic world and afford them better protection against many types of cybercrime, such as phishing and identity theft.[414] The German eID deployment should also be understood in relation to Germany's participation in the EU Stork project, which aims to establish a European eID Interoperability Platform that allows citizens to establish new e-relations across borders, just by presenting their national eID.[415]

Proponents of the card envision that it can replace username and password, and at the same time allows services previously requiring the presence of the citizen to be provided electronically.[416] The specific design rationale is driven by a number of goals:

- Easier online authentication with more control and responsibility given to the citizen;
- Reliable authentication and high quality data records available to the service providers;
- Data reduction and data economy through designing the eID system according to the need-to-know principle;[417]
- No centralized databases of personal information;
- Privacy enhancement through the support of pseudonyms and on-card data verification;
- Protection against threats through protocol design;
- User control – entering a PIN is a requirement to grant access to any data or function.[418]

Services that might especially benefit from supporting eID are government services requiring identification of citizens, services allowing citizens to access personal information, companies required to record identities of their customers and operators of age-restricted services.[419]

Relevant Actors

The responsibility for the implementation and operation of the eID system is shared between the government and the private sector. Local administrative bodies register citizens and issue ID cards, Federal administrative agencies issue authorizations to service providers and oversee equipment certifications[420] and private parties participate as service providers, deliver specific technical elements of the eID infrastructure or as users. The following are the most relevant actors involved in the governance of information infrastructures protection:

[413] BSI (Bundesamt für Sicherheit in der Informationstechnik) (2010), *Innovations for an eID Architecture in Germany,* Bonn: BSI., p. 4.
[414] BSI (2010), p.5.
[415] See: https://www.eid-stork.eu/
[416] Poller et al. 2012, p. 48.
[417] Service providers are authorized to access only data that they can demonstrate to have a real need for.
[418] Poller et al. 2012, pp. 51-52.
[419] Poller et al. 2012, pp. 48-49.
[420] Poller et al. 2012, p. 50.

- Federal Office for Information Security (BSI: Bundesamt für Sicherheit in der Informationstechnik) is a key player in the operation of the eID. It is affiliated to the Federal Ministry of Interior under the guidance of the IT Group.[421] It issues the technical guidelines for certification of all components of the eID system and operates the Country Verifying Certificate Authority (CVCA). This authority generates the German root certificates on a regular basis and the BSI is the owner of these root certificates for authorization certificates for electronic identification.[422] The BSI is also in charge of developing security protocols and measures[423]. The BSI falls under the Federal Ministry of Interior (see Chapter 4).
- Federal Office of Administration (BVA: Bundesverwaltungsamt) approves service providers that have a legitimate interest in using eID data and comply with all regulations. It also provides ID card revocation lists to eID servers.[424]
- Technical Certification authorities contract with service providers and issue cryptographic authorization certificates to them for the respective eID servers.[425]
- The Federal Print Office (Bundesdruckerei GmbH) is assigned the role of the ID card manufacturer by the Federal Ministry of Interior.[426]
- Local agencies issue ID cards produced by the Bundesdruckerei to citizens. These ID card public authorities, appointed by the German Länder authorities, in accordance with § 7 para. 1 PAuswG, are responsible for matters related to identity cards[427] and are obliged to explain the eID process to the card holders, deliver the letter with the original PIN[428] and handle revocation requests by the card holders.[429]
- Service providers are either public offices or online retailers that require proof of identity of the identity card holder in order to carry out tasks of the public administration or for own business purposes,.[430] Insofar as they are using contractors they have to do this in accordance with the Data Protection Act (see below) and that these contractors meet the technical and organizational requirements of the BSI.[431]
- Local data protection authorities are responsible for service providers in Germany.[432]
- eID servers may be operated either by the service providers themselves or by a contracted eID service provider. These servers perform communication with the client software and handle communications for requesting certificates.[433]

[421] T Noack and H Kubicek, ‘The introduction of online authentication as part of the new electronic national identity card in Germany’ (2010), pp. 102-103.
[422] BSI (2010), p. 15.
[423] §32 PAuswV.
[424] Poller et al. 2012, p. 50.
[425] Poller et al. 2012, p. 50 also §33 PauswV.
[426] G Hornung and A Roßnagel 2010, p. 151.
[427] §7(1) PAuswG.
[428] Only, if the applicant requests delivery through the ID card authority, otherwise it is sent by the card manufacturer (§13 PAuswG).
[429] §4 PAuswV.
[430] §2(3) PAuswG.
[431] §29(4) PAuswV.
[432] §7(5) PAuswG.
[433] BSI (2010), p. 19.

- Client software providers provide the software needed for communication between the citizen's ID card (reader) and eID server AusweisApp is free software available for download on the portal of the Federal Ministry of Interior, which funded its development[434] by OpenLimit SignCubes AG commissioned by Siemens IT Solutions and Services GmhB. Other alternative software clients may also become available on the market.
- Individual users are also critical to the secure operation of the eID infrastructure. They indicate whether or not they want to use the eID function[435], are informed of the measures necessary to ensure its safety[436] and are required to ensure that electronic identification is used in a safe environment. They are also required to re-set the original PIN[437] and indicate the loss of ID card to the ID card authority.[438]

Regulatory Framework

In the E-Government Act – E-Government-Gesetz – the eID and the online Ausweis function were established as one of the instruments for safe e-government at the federal, state and local levels. The legal framework for identity documentation in general and for electronic proof of identity specifically is provided in the German ID Card Act - Gesetz über Personalausweise und den elektronischen Identitätsnachweis (PAuswG 2010). The corresponding sub-statutory regulation Verordnung über Personalausweise und den elektronischen Identitätsnachweis (PAuswV 2010) defines the security and data protection requirements of the eID infrastructure. This framework is complemented by almost 20 technical guidelines and profiles of protection prescribed by the Federal Office for Information Security (BSI) published in binding form in the Federal Gazette. This set of legislation aims to provide comprehensive coverage and regulation of all aspects of the e-ID infrastructure. Other laws, such as the Federal Data Protection Act (Bundesdatenschutzgesetz) or the BSI-act, are only relevant insofar as there are still gaps in the PAuswG and related sub-statutory regulation.

Similar to the other country descriptions, this text is structured according to three categories: regulation of prevention, regulation of incident management and regulation of repression. As will become apparent, the first category has been the dominant driving force of the German regulatory approach, where incident prevention is achieved through the technological design of the e-ID infrastructure.

Regulation of Prevention

The protection of data, data security and preservation of informational self-determination are listed as particular priorities of the electronic ID infrastructure.[439] Using the eID function is voluntary for

[434] See: https://www.ausweisapp.bund.de/startseite/
[435] §10 PAuswG.
[436] §11(3) PAuswG.
[437] §23 PAuswV.
[438] §27(3) PAuswG.
[439] See: http://www.personalausweisportal.de/SharedDocs/Downloads/DE/Flyer-und-Broschueren/eID_Broschuere.pdf;jsessionid=234460B7B81F96B9060A8BAC3CEF7DB2.2_cid289?__blob=publicationFile 11-12.

the card holder[440] in a double sense: they can decide to switch it on and off, and they can decide upon using it in concrete individual cases.[441] User data is only exchanged between the service provider and the holder of the identity document. Biometrically-relevant data are never transmitted via the internet and only sovereign authorities are authorized to access such sensitive information.[442]

Since the German constitution does not allow the creation of a unique identification number,[443] individuals are identified by a combination of attributes. The authorized eID servers can access the following data on the ID card on the basis of selective disclosure: family name, given name, artistic or religious name, doctoral degree, date and place of birth, address and community ID, date of expiry and revocation feature.[444] The eID function also supports a privacy- enhancing mode where, instead of the specific age or place of residence, the card only responds yes/no to a verification request.[445] An additional data protection friendly feature is the service and card specific code (pseudonym) which allows for the possibility of non-linkable logins (in the absence of other identifiers).[446]

Before being able to access personal data stored on the ID card chip, institutions are legally required to possess an appropriate authorization, which depends upon a review by the government authorities of which data the service provider absolutely requires for her purposes and whether she is trustworthy. The authorization is technically implemented using authorization certificates, whose status is queried at terminal authorization. The ID card releases data to a service provider only upon displaying an authorization certificate[447] that proves the identity of the service provider and shows which data it is authorized to read.[448] The holder of the card may also restrict access to specific eID data fields via the client software. Therefore, the citizens are also able to authenticate the service provider and check its data requests, forming double-sided, mutual authentication required by law in Germany.[449] The release of the data to the service provider is also conditioned by the entering of a six-digit PIN by the ID card holder. [450] Entering the PIN incorrectly three times deactivates the function and reactivation requires the Entsperrnummer (PUK).[451]

Technically, the use of the ID card online is enabled by software called ‘AusweisApp’ (‘another alternative software solution’) which serves as the interface between the ID, the card reader and the eID server of the service provider.[452] All of these eID components require

[440] §10(1) PAuswG.
[441] Hornung and Roßnagel 2010, p. 154.
[442] BSI (2010), p. 5.
[443] OECD (2011), p. 48.
[444] §18(3) PAuswG.
[445] Poller et al. 2012, p. 48.
[446] GL Rosner, ‘*Identity management policy and unlinkability: A comparative case study of the US and Germany*’ (PhD Thesis, University of Nottingham 2014), p. 182.
[447] BSI (2010).
[448] §2(4) PAuswG
[449] Noack and Kubicek. 2010, p. 98.
[450] M Horsch, J Braun, and A. Wiesmaier ‘Mobile eID Application for the German Identity Card’ (Technical Report, Technical University Darmstadt 2013), p. 3.
[451] §2(12) PAuswG.
[452] See: https://www.ausweisapp.bund.de/startseite/

certification from the BSI.[453] The software is provided free of charge on the web portal of the German Federal Ministry of the Interior.[454] Basic card readers leave all control over the user interaction to the software, while advanced readers have their own keypad for entering the PIN.

The PAuswG requires that the transmission of data is subject to state of the art measures ensuring data protection and data security.[455] A number of security protocols and measures were developed under the leadership of the BSI in order to achieve the security objectives of protection of personal data, proof of the authenticity of the identity document and proof against forgery.[456] The protocols ensure that data are released only with card holders' consent, to an authorized service, within the authorization limits and through channels protected against eavesdropping.[457]

- Password Authenticated Connection Establishment (PACE) establishes a shared session key and verifies a password in the process. [458] The 6-digit PIN is used during online authentication.[459]
- Extended Access Control (EAC) comprises an array of protocols that are always executed in a specific order. The EAC protocols include Chip Authentication (CA), the purpose of which is to confirm that the chip is a real one and to establish a secure communication between the chip and the reader or between the chip and the service provider during online authentication, and Terminal Authentication (TA), which ensures that sensitive data can only be read by authorized persons.[460]
- The purpose of Passive Authentication (PA) is to validate the authenticity and integrity of the data on the chip and whether the data in the identity document were written on the RF chip by the officially authorized ID manufacturer.[461]
- Restricted identification (RI) cryptographically creates identifiers that are specific to the card and to the service and cannot be linked.[462]

The BSI also operates the Country Verifying Certificate Authority (CVCA). This authority generates the German root certificates on a regular basis; the private keys of these certificates are used to sign the document verifier certificate of the document verifier instances (DV instances).[463]

Simplifying the use of eID function in web application is achieved by the eID servers, which provide a simple interface encapsulating the complexity of the eID function. The eID server establishes communication with the AusweisApp and handles the communication for requesting terminal authorization certificates, CSCA certificates and revocation lists. The eID server operates as a logically independent server which can be used by multiple web applications. The data

[453] §23(2) PAuswV.
[454] See: https://www.ausweisapp.bund.de.
[455] §18(2) PAuswG.
[456] BSI (2010), p. 9.
[457] Poller et al. 2012, p. 49.
[458] Poller et al. 2012, p. 48.
[459] §2(10) PAuswG.
[460] BSI (2010), pp. 11-13.
[461] BSI (2010), p. 15.
[462] Poller et al. 2012, p. 48.
[463] See: https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/CVCAeID/CVCAeID_node.html

transferred between the eID server and the application server via a public network must be encrypted and signed for transfer.[464]

Regulation of Incident Management

The regulators seem to rely strongly on the technological solutions of the eID infrastructures to prevent security incidents, whereby the management of security incidents does not appear to be extensively regulated. The only potential vulnerability of the eID infrastructure that is specifically addressed in legislation is loss of ID card by the user; the PAuswG specifies the steps that need to be taken in such a case. The card holder must report loss of the ID card to the ID card authority,[465] who immediately informs the administrator of revocation lists. The administrator provides current revocation lists to all service providers in the system. The card holder can also contact the administrator of revocation lists directly.

Other potential security incidents or vulnerabilities of the eID infrastructure were pointed out by activists before its launch in 2010. One criticism related to the basic card readers (without their own keyboard) that were distributed for free by the government, which made them vulnerable to malicious software such as keyloggers that could record the PIN entered by the user. The BSI deflected this criticism by pointing out that even if a criminal obtained the PIN, it would be useless without physically having the ID card.[466] The critics further claimed that even without possession of the card, the criminal could abuse an obtained PIN if the user left the ID card in the proximity of a card reader for longer than necessary. This concern was recognized by the BSI, but it pointed out that the attacker could still not obtain personal data due to its encrypted form and – even with such vulnerability – the new system is still more secure against attacks than an alternative system based on a username and password.[467] Nevertheless, the use of the more expensive advanced card reader with a keypad is recommended.[468] However, other groups questioned and successfully challenged the security of these more advanced card readers, as well.[469] Similar concerns about the vulnerability of the PIN codes were raised in 2013.[470]

Another potential vulnerability stems from the decision of the designers of the German eID infrastructure. To protect users' privacy, a batch of ID cards always shares the private chip authentication key which makes them indistinguishable at the protocol level. If an attacker obtained this key in some way, it would allow him/her to forge new identities and the eID servers could not

[464] BSI (2010), p. 15.

[465] §27(1)3 PAuswG.

[466] 'Missbrauch der elektronishen Ausweisfunktion nicht möglich', http://www.golem.de/1008/77473.html accessed 6 June 2015.

[467] 'CCC zeigt Sicherheitsprobleme beim elektronischen Personalausweis auf', http://www.heise.de/newsticker/meldung/CCC-zeigt-Sicherheitsprobleme-beim-elektronischen-Personalausweis-auf-Update-1083649.html accessed 6 June 2015.

[468] Poller et al. 2012, p. 48.

[469] 'Wietere Angriffe gegen den nPA', http://www.golem.de/1012/80347.html accessed 6 June 2015.

[470] 'Chaos Computer Club wieder sicherheitsluecke im Elektronichen Personalausweis', http://www.golem.de/news/chaos-computer-club-wieder-sicherheitsluecke-im-elektronischen-personalausweis-1308-101214.html. accessed 6 June 2015.

recognize spoofed cards. While this could be solved by revocation of the compromised key, this would simultaneously render many cards unusable in eID.[471]

Soon after the adoption of the eID infrastructure in November 2010, the client software for e-ID (AusweisApp) was withdrawn due to vulnerability in the automated update function. A new version of the software was provided less than two month later.[472] However, during this research, we did not encounter report of a specific security incident where a vulnerability was abused.[473]

Regulation of Repression

Due to the strong reliance on the security of the e-ID technological design and the perceived lack of security incidents, repression is not specifically dealt with in the e-ID legislation. We can assume that a number of provisions of the Criminal Code (StGB – Strafgesetzbuch) would apply to possible actions of perpetrators against the e-ID infrastructure and its users: unlawfully obtaining data for oneself that were intended for someone else and were especially protected against unauthorised access (§202a StGB), unlawful interception of data not intended for oneself by technical means from a non-public data processing facility or from the electromagnetic broadcast of a data processing facility (§202b StGB), computer fraud defined as damaging property of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorised use of data or another unauthorised influence on the course of the processing with the intention of obtaining unlawful material benefit (§263a StGB), forgery (§267 StGB) and forgery of data intended to provide proof for the purposes of deception in legal commerce (§269 StGB), tampering with official identity documents (§273 StGB), acquisition of false official identity documents (§276 StGB) and misuse of identity documents defined as using, for the purpose of deception in legal commerce, an identity document issued to another (§281 StGB).

It is noted in literature that the possibility of the cardholder to validate the identity of an interaction partner given by the authorisation certificate makes the prosecution and law enforcement easier (or at least possible) if a legal dispute arises.[474]

5.2.4 The Netherlands

In the Netherlands, electronic identities are issued via a number of routes. Citizens can make use of DigiD, businesses can make use of eRecognition *(eHerkenning)* and for machine-to-machine communication and between government agencies there is PKI-government (Public Key Infrastructure-government). There are also numerous organisation-specific solutions. In the (near) future, the three identity infrastructures (DigiD, eRecognition and PKI-Government) will be brought

[471] Poller et al. 2012, p. 51.
[472] See: http://www.golem.de/1101/80433.html.
[473] The lack of occurrence of specific security incidents was also confirmed in an interview with Prof. Dr. Gerrit Hornnung from the University of Passau (conducted on 15 June 2015 via Skype).
[474] Hornung and Roßnagel 2010, p. 155.

together in the so-called e-ID infrastructure.[475] Because various aspects of the e-ID redesign have yet to be clarified and are under development, it is not further discussed here.

For the purposes of this report, the identity focus is on the three services of DigiD: 1) DigiD, which is the default service; 2) DigiD Machtigen, which gives one citizen the authority to act on behalf of another citizen and 3) DigiD Balie, which allows a citizen to obtain a DigiD by going to a physical desk, rather than online (which is the 'normal' procedure). DigiD services are available with three levels of security that are based on which authentication measures are used, namely: DigiD security level Basic (username and password), DigiD security level Medium (username, password, and SMS authentication), and DigiD security level High (qualified electronic signature) (art. 1(9) CD). The customer (i.e. organization that uses DigiD to identify citizens) is responsible for determining the desired Security level for its Customer services (webservices) (art. 5(1) CD).

DigiD is an interesting case to consider, despite pending changes, because there have been several recent security incidents related to DigiD that reveal important insights for cybersecurity governance. In 2011, large-scale fraud with applications for child-care, rent and health insurance allowances was revealed.[476] It appeared that the tax authorities allowed these applications to be signed with any DigiD (and not just with the applicant's DigiD) because many people find it hard to comply with the formalities of these applications and this enabled them to ask a friend or relative to complete the application on their behalf. Fraudsters used a random DigiD to apply in someone else's name and to change the number of the bank account to which the advances would be paid. After many complaints about fraud, the tax authorities brought about changes and now they check that the DigiD used to sign an application belongs to the applicant.

A second case occurred in September 2014, when a software company reported to the administrator of DigiD that there was vulnerability in its Content Management System (CMS). An investigation showed that in 12 municipalities, the connection between CMS and DigiD was set up in such that there was a risk of abuse. According to the software company, the vulnerability was rectified within 24 hours after discovery with the development and application of a patch for the affected municipalities. The software company informed the municipalities involved; as far as is known the vulnerability was not exploited.[477]

Then, in October 2014, two people were arrested by the FIOD for fraud with DigiDs through which they robbed about €50,000. They used the usernames and passwords of others to access and adjust bank accounts and telephone numbers on government websites in order to steal (among others) social security benefits (AOW). Approximately 5,000 DigiDs were used without authorization and for approximately 180 DigiDs, coupled data were altered. Four others were

[475] More information on the eID infrastructure can be found on <http://www.eid-stelsel.nl/> accessed 13 May 2015.

[476] T Verkade, 'Massafraude met belastingtoeslagen via DigiD' *NRC* (19 September 2011). <http://www.nrc.nl/nieuws/2011/09/19/massafraude-met-belastingtoeslagen-via-digid/> accessed 13 May 2015.

[477] Kamerstukken II, 2014-2015, Handelingen Aanhangselnummer 515, Gepubliceerd op 11 november 2014, Vragen van de leden Oosenbrug en Fokke (beiden PvdA) aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties over een lek in DigiD (ingezonden 30 oktober 2014). Antwoord van Minister Plassterk (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 10 november 2014).

arrested for possibly functioning as ‘money mules’, persons who provide bank accounts for depositing money that has been obtained through fraud. The money was never on the bank accounts for long as it was immediately withdrawn in cash. In many cases, the relevant government body could intervene in time or reverse operations. The citizens concerned were informed immediately and the 5,000 compromised DigiDs removed. The approximately 70 suspicious bank accounts emerged from the investigation have been blocked by the banks. The damage was kept relatively limited because the government services detected the fraud quickly.

The Dutch government encourages citizens through various campaigns to act carefully with their DigiD account and never asks for personal information via e-mail of telephone. According to the government, every possible action is taken to secure the use of DigiD and prevent phishing. In the following section, we identify the relevant actors that contribute to this effort.

Relevant Actors

This section describes the actors directly involved with DigiD:

- The Ministry of the Interior and Kingdom Relations is responsible for the policy on the DigiD facilities: DigiD, DigiD Machtigen and DigiD Balie. The Ministry commissioned Logius to manage these facilities and plays the role of owner. Logius outsourced the production of the facilities to the market.
- The Ministry of Economic Affairs also commissions tasks to Logius regarding the network of eRecognition. [478]
- Logius[479] is the service for digital government and an agency of the Ministry of the Interior and Kingdom Relations**.**[480] Logius develops services and standards for the entire Dutch government and is responsible for the administration, development and application of these services[481] and standards. Logius is advised by the Programme Council (Programmaraad***)**,* which is an advisory body consisting of Logius customers. Logius supports the Dutch Minister of Interior and Kingdom Relations with the management and control of the PKI-overheid system.[482] Logius is not only the administrator of the DigiD system; it is also the actor who issues DigiDs to citizens/users.
- Reliant organisations: Many government institutions and agencies use DigiD to identify citizens and carry out various services and tasks. Examples include the Dutch provinces and municipalities; the Dutch Tax Authority *(Belastingdienst)*; the IB-Group; the Dutch unemployment service *(*Uitvoeringsinstituut Werknemersverzekeringen, *UWV)* and the Social Insurance Institute *(Sociale Verzekeringsbank, SVB)*. Conform the terminology of the contracts governing DigiD, these organizations are called ‘customers’. Via DigiD, these

[478] C Cuijpers, ‘Country report eID in the Netherlands’ (Working paper, 2014), paragraph 3.2.

[479] See https://www.logius.nl/

[480] In Dutch law, an agency is an independent, organisational entity within a ministry. See <http://www.parlement.com/id/vh8lnhrqszxe/agentschappen_baten_lastendiensten> (in Dutch) accessed on 13 May 2015.

[481] See https://www.logius.nl/diensten/

[482] Ibid, paragraph 3.3.

organizations can obtain an individual citizen's *(ingezetenen)* Social Security Number (SSN), and with the SSN as a key, additional information from the Key Registry Persons (Basisregistratie personen, BRP).[483] They can also obtain information on persons living in other countries who are related to the Dutch government (*niet-ingezetenen).* People can check which organizations use their personal data and for what reasons on www.wiekrijgtmijngegevens.nl.[484]

- Suppliers: Logius is the administrator but does not build the technical infrastructure itself. This is outsourced to commercial companies. In this report, they are called the suppliers.
- The State Audit Service (*Auditdienst Rijk, ADR)* is the government service involved in the oversight of Logius and the suppliers.
- End-users: An end-user is defined as natural person who is registered in the Municipal Records System (*Gemeentelijke Basisadministratie Personen,* GBA), who has a social security number or another number issued by government and who has applied for a DigiD (art. 1.5 Terms and Conditions of Use DigiD). As citizens, they need to provide certain types of information to the government; some data are automatically generated or changed in the KRP, for example when you get married in the Netherlands. As end-users, they can also help increase safety by using DigiD carefully and following the advice of Logius. The running Alert Online campaign also has a strong focus on Internet safety, for example via the website www.veiligInternetten.nl[485]

Regulatory Framework

There is no strong basis for DigiD in legislation. Its regulation is mainly based on private law instruments, such as contracts or on rules governing the use and accessibility of data from the BRP, which is regulated by the Key Registry Persons Act (Wet Basisregistratie personen).[486] Similar to the approach taken in Chapter 4, we distinguish between regulation of prevention, regulation of incident management and regulation of repression (for the full explanation see Section 4.1.3).

Regulation of prevention

Ministerial control of Logius and connected organisations

The Ministry as owner monitors whether the parties connected to DigiD comply with the requirements outlined in the Connection Conditions DigiD Single Logon *(Aansluitvoorwaarden DigiD Eenmalig inloggen)*. The Ministry's role of supervisor on the DigiD facilities has not been fully developed. Therefore, in practice, administrator Logius also performs monitoring duties (see below under Connection Conditions).

[483] Basisregistratie personen (BRP); See: http://www.rijksoverheid.nl/onderwerpen/persoonsgegevens/basisregistratie-personen-brp> accessed on 13 May 2015.

[484] This is the 'WhoObtainsMyData' website.

[485] This is the 'SecurelyUsingInternet' website.

[486] <http://wetten.overheid.nl/BWBR0033715/geldigheidsdatum_07-04-2015> accessed 13 May 2015.

The ministerial responsibility of the Minister of the Interior and Kingdom Relations extends fully over Logius. Each year, ADR audits the technical implementation and management processes of the suppliers as well as the management processes of Logius concerning DigiD and DigiD Machtigen. The assessment is governed by the Logius framework for general administrative processes *(Logius normenkader voor generieke beheerprocessen)*. The framework is based on the NOREA framework for IT administration processes.[487] Information protection plans for DigiD facilities contain the analysis of the security risks and the specification of the protective measures. The risk analysis and defined measures are source materials for the judgment of the ADR and the assessment of Logius of the implementation of the security measures by the supplier.

The Ministry can enforce compliance with the agreements and norms governing DigiD in the following ways: 1) allowing Logius to cut off a connected party; 2) at the request of Logius, addressing a connected party, for example, by way of a formal letter to the board and 3) dissolving Logius' assignment to administrate DigiD facilities.

Relationship between Logius and customers

This relationship is governed by contractual conditions, such as the General Conditions of Logius, the Conditions DigiD and the Connecting Conditions DigiD Single Logon.

Conditions DigiD (CD)

The Conditions DigiD are applicable in the relationship between Logius and any organisation using DigiD to identify citizens (the 'customer') and hold in addition to the General Conditions Logius.[488] The General Conditions of Logius define a customer as 'a public or private organization, or a board or a person that deems electronic communication with other governmental bodies and citizens and/or companies desirable for the execution of a public task, and that for that purpose can and may use one or more of Logius' services (art. 1.2 GCL).

Every connected organisation must undergo an annual 'DigiD assessment' by an independent registered EDP auditor (art. 5(5) CD). Organizations that connect for the first time to DigiD must complete the assessment successfully within two months after connection (art. 5(6) CD). The assessment is governed by the *Norm ICT-beveiligingsassessments DigiD*,[489] the security norm established by the Ministry of the Interior and Kingdom Relations (art. 1(7) CD), which is based on the ICT-beveiligingsrichtlijnen voor webapplicaties (ICT Security guidelines for web applications) of the NCSC.[490] Other relevant norms specifically for DigiD and DigiD Machtigen are the 'Logius normenkader voor DigiD' (Logius Framework for DigiD) and 'Programma van Eisen (ten dele) voor DigiD' (Programme of Requirements (partly) for DigiD). For DigiD Balie, the 'Logius

[487] NOREA is the Dutch Order for EDP registered accountants, see <www.norea.nl> accessed on 13 May 2015.

[488] General Conditions Logius: <https://www.logius.nl/fileadmin/logius/ns/diensten/algemeen/20120401__Algemene_voorwaarden_Logius_versie_1_0.pdf> accessed on 13 May 2015.

[489] https://www.logius.nl/fileadmin/logius/ns/diensten/digid/assessments/120221_norm_ict-beveiligingsassessments_digid.pdf (accessed on 13 May 2015).

[490] Framework ICT protection assessments for the DigiD: <https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html> accessed on 13 May 2015.

normenkader specifiek voor de uitgifteprocessen en de onderliggende infrastructuur bij de uitgifte balies' is relevant (Logius Framework specifically for issuing processes and the underlying infrastructure of the issuing desks).

The audit report is sent to Logius that assesses the report.[491] If the report shows that an organization does not (completely) comply with the Norm ICT-beveiligingsassessments DigiD Logius can suspend its DigiD services without prior notice (art. 5(9) CC). Logius can enforce the compliance with the relevant norms and agreements by discussing the risks of non-compliance with the connected party, formally addressing the connected party cutting off the connected party in case of an immediate security risk due to vulnerable implementation, or referring to (or dissolving) the contract with suppliers of the infrastructure of DigiD.

The Connection Conditions Single Logon (CCSL)[492]

These conditions apply to the relationship between Logius and any organisation (customer) using DigiD to identify citizens by a single log-on. CCSL is an addition to the Connection Conditions for the Single-Logon-use of DigiD whereby the authentication of the users is reused, so that a user need not login anew during a session. In the so-called 'Handreiking DigiD', Logius prescribes the security means and measures that the customer has to take (art. 6(1) CCSL). A customer is responsible for the security of its own decentred technical infrastructure (art. 6(2) CCSL). If Logius adapts its security requirements, the customer is granted a reasonable term to realise the necessary technical changes. If the customer does not conform to Logius' requirements, Logius can suspend or terminate the use of computer programs or services (art. 6(3) CCSL). Logius will take technical and organisational measures to protect personal data from loss or any kind of unlawful processing. These measures need to be appropriate, considering the state of technology and the associated costs, and focus on the prevention of unnecessary collection and processing of personal data (art. 7(1) CCSL).

With regard to the Single Logon Function, customers are mutually dependent on the reliability and security of their systems and are obliged to Logius and the other customers to take technical and organizational measures that ensure that the identity of the user leaving the service corresponds to the identity provided by the Single Logon Function (art. 6(1) CD).

Use Conditions[493]

These conditions apply to the relationship between Logius and an end-user. The end-user is bound to a few security related obligations, such as confidentiality of the DigiD (art. 2.9 UC). Furthermore, the e-mail address and telephone number that the user issues to Logius must belong to an e-mail

[491] The statement has to be handed in at Logius between the first of January and the first of May (art. 5(5) Conditions DigiD).

[492] Connection Conditions DigiD Single Logon *(Aansluitvoorwaarden DigiD Eenmalig Inloggen)*: <https://www.logius.nl/fileadmin/logius/ns/diensten/DigiD/voorwaarden/101122_Aansluitvoorwaarden%20DigiD%20Eenmalig%20inloggen%20v1.0.pdf> accessed on 13 May 2015.

[493] Conditions DigiD: <https://www.digid.nl/voorwaarden/#c348> accessed on 13 May 2015. For the service DigiDMachtigen additional terms and conditions apply: https://www.digid.nl/machtigen/gebruiksvoorwaarden/.

account and cell phone that is under the user's control (art. 2.12 & 2.10 UC). If the user knows of abuse, loss, theft or any other mishap to the issued DigiD, he should immediately report this to the Helpdesk DigiD. Logius will do its best to block the DigiD as soon as possible (art. 6.4 UC). In case of (suspected) abuse or misuse of DigiD Logius may decide to exclude the user from further use of DigiD (art. 2.15 UC).

Apart from binding users to contractual security-obligations, Logius also provides security related information to users. Logius gives for example tips on how to make a safe password, how to recognize, stop and notify abuse of DigiD, and how DigiD itself tries to ensure its safety.[494]

Regulation of Incident Management

Conditions DigiD

A security incident is an event that is or can be a threat to the reliability, confidentiality or availability of DigiD (art. 2.3 CCSL & art. 1.4 General Conditions of Logius, GCL). Logius has the right to suspend the delivery of services temporarily and without announcement in case of a security incident (art. 5.4 GCL).

Bill on Cyber Security Data Processing and Reporting of Incidents

It is unclear whether Logius will fall under the Bill on Cyber Security Data Processing and Reporting of Incidents. In the CMS-incident described above, Logius informed the NCSC, the information security service of municipalities (IBD) and the Ministry of the Interior and Kingdom Relations about the vulnerability and the solution chosen.

The Logius Calamity Plan

This plan became public through a Freedom of Information Request. It contains detailed information about the escalation of incidents, communication in the event of an incident and performance indicators for the resolution of problems.[495] Escalation basically relates to "when do you warn your boss". There is a classification of incidents, whereby functionaries with increasingly more authority and powers need to be called upon as an incident becomes more serious. The calamity plan indicates what to do and when and stipulates the rules about communication. These rules build on three starting points: 1. accuracy of communication, 2. honesty and timeliness of communication and 3. internal communication before external communication. The performance indicators of the calamity plan indicate, for example, how fast an incident needs to be resolved. Naturally, incidents with a high priority need to resolved more quickly (e.g. within 8 hours) than lower priority incidents (e.g. within 2 working days).

[494] See for example: <https://www.digid.nl/veiligheid/ accessed 13 May 2015.>

[495] Available at: <http://webcache.googleusercontent.com/search?q=cache:smk9OjsagmwJ:www.rijksoverheid.nl/bestanden/documenten-en-publicaties/wob-verzoeken/2011/11/16/wob-verzoek-over-het-calamiteitenplan-van-logius/te-publiceren-stukken-wob-verzoek-inzake-calamiteitenplan-logius.pdf+&cd=1&hl=en&ct=clnk&gl=nl> accessed on 13 May 2015.

Regulation of Repression

As the introductory examples showed, DigiD incidents may come in various forms of unauthorised use or other systemic breakdown. The 'normal' criminalizations in the field of computer crime can be used to prosecute these offenses. The Computer Crime Act (1993) and the Computer Crime Act II (2006) have added relevant provisions to the Criminal Code. A Computer Crime Bill III is in preparation, which will inter alia criminalise receiving (*heling*) of data. The legislation implements the international obligations to criminalise computer offenses of the Convention on Cybercrime and Directive 2013/40/EU.

The purpose of manipulations in electronic identity systems is often financial gain. Therefore, perpetrators may also be prosecuted for financial-economic crimes such as fraud (art. 326 DCC) or forgery (art. 225 DCC). Many of the criminalizations in this field are sufficiently technology-neutral to allow their applications in electronic environments. The punishments that can be imposed on perpetrators are also relatively high. It is questionable whether specific identity-related offences such as forgery of an identity document (art. 231 DCC) or forgery of an identity card (art. 232 DCC) are applicable to DigiD. However, in 2014, a new provision was included in the Criminal Code that penalises the unlawful use of someone else's identifying personal data with the purpose of hiding one's identity or of hiding or abusing someone else's identity, if this can result in any harm; this is punishable with up to five years' imprisonment (art. 231b DCC).[496] This can address most unlawful uses of other people's DigiD; it does not, however, cover situations in which people use fake DigiDs.

5.2.5 United Kingdom

Digital identity is fundamental to the development of e-government initiatives. As stated jointly by CESG, the National Technical Authority on Information Assurance[497], and Cabinet Office's Government Digital Service, "within the UK there is no official or statutory attribute or set of attributes that are used to uniquely identify individuals across Government. Neither is there a single official or statutory issued document whose primary purpose is that of identifying an individual."[498] Identification credentials seem to be a peculiarly sensitive matter in the UK: identity cards,[499] for example, were abolished[500] in 2011 by the Identity Documents Act 2010 (c. 40) and the personal data of every identity card holder were erased from the government's national identity register. Citizens, however, arguably benefit from secure authentication, especially in relation to online government services. Conversely, e-IDs sensibly reduce the cost governments must undertake to provide their services, while, "benefits to users are a reduced risk of fraud, increased convenience and reassurance that they are interacting with a bona fide service."[501]

[496] Staatsblad 2014, 125.

[497] Formerly 'Communications-Electronics Security Group'.

[498] CESG, Cabinet Office, 'Good Practice Guide No. 45 – Identity Proofing and Verification of an Individual' (Issue No 2.3, 2014), p. 3.

[499] Originally introduced by the Identity Cards Act 2006 (c 15), now repealed.

[500] See https://www.gov.uk/identitycards.

[501] Parliamentary Office of Science & Technology (POST), 'Managing Online Identity' (Postnote Number 434, 2013), p. 4.

Currently, a federated approach to identity is emerging: a public service provider engages in online transactions with a subject whose identity is verified and authenticated by a third party[502], the Identity Provider. The subject can use the credentials provided by an Identity Provider with a multiplicity of service providers, and has the possibility to choose between different identity credentials if more than one Identity Provider verifies his identity. A federated identity system should ensure that the technologies used, the processes deployed, and the parties on which they rely are secure and trustworthy. This is achieved through a combination of technical and business elements and legal and contractual rules.

Relevant Actors

The following actors are relevant to the governance of identity infrastructures in the UK:

- The Government Digital Service in the Cabinet Office runs a federated identity program called Identity Assurance Programme (IDAP), in the context of its Digital Transformation Programme,[503] which aims at implementing the governmental "digital by default" policy. Its purpose is to develop a framework for ensuring that the electronic credentials representing a person accessing and signing in a number of governmental online services actually identify that person with some level of certainty, which will be referred to as Identity Proofing and Verification (IPV).
- The Communications Electronics Security Group (CESG) is the Information Security arm of GCHQ (see Chapter 4). It is the National Technical Authority for Information Assurance within the UK. It states that it is "the definitive voice on the technical aspects of Information Security in Government."[504] CESG has a leading role in providing the relevant stakeholders with guidance, standards and best practices.
- Service providers deliver various e-government services in the UK; in order to use them, citizens need to identify themselves through an identity provider.
- Identity providers are organizations paid by the government to identify the citizens that use their services. Once an identity provider has positively identified a citizen, the latter can use the former for authentication when accessing a given service provider. The IDAP uses a technical intersection (hub) that allows identity providers to confirm the identity of the service user to the GOV.UK service provider without the government centrally storing an individual's data, without unnecessary data being exchanged and without either party sharing users' data stored in their servers.[505]

[502] The very basis of identity management are the processes of identification (issuing an identity credential to an individual or an organisation that claims it) and authentication (verifying that the claimed identity does indeed belong to that person or organisation): see Thomas J Smedinghoff, 'Solving the legal challenges of trustworthy online identity' (2012) 28 Computer Law & Security Review 532.

[503] See https://www.gov.uk/transformation.

[504] https://www.cesg.gov.uk/AboutUs/Pages/aboutusindex.aspx.

[505] See Cabinet Office and Government Digital Service, 'Identity assurance: delivering trusted transactions' (2014) https://www.gov.uk/government/collections/identity-assurance-enabling-trusted-transactions, last access June 2015.

Regulatory Framework

There seems to be no clear-cut legal basis for the Gov.UK identity verification framework in current legislation: its regulation is mainly based on private law instruments and good practice guides issued by the CESG.

Regulation of Prevention

PCAG Identity Assurance Principles

The Privacy and Consumer Advisory Group (PCAG) was established as an independent working group in order to develop a framework for the IDAP to be built upon. The PCAG elaborated, after a public consultation process, a set of nine principles to be applied in the context of identity assurance. The principles currently stated in their third edition:[506]

1. User Control: The IDAP services can be performed only with the consent and approval of the service user; no compulsion can be exercised to undermine the user's free choice, so means of identification alternative to IPVs have to be provided.
2. Transparency: The user has to be fully informed in advance and in a way that is clear and understandable to him. The way in which the data is processed and the authentication services provided must be transparent to him. Any significant change to the processing arrangements that have been previously described to a service user requires its prior consent. Moreover, all procedures, including the security ones[507], should be made available unless their publication represents a risk to users security or privacy.
3. Multiplicity: Service users are free to use any number of identifiers, to use any identity provider and any number of service providers they wish, and to change provider at will. If a user registers with more than a service provider, it is forbidden to those providers to exchange information between them.
4. Data Minimisation: The amount of data to be used is the minimum necessary to achieve the user's needs. Identity assurance itself should be used only where there is an established need. Once a user stops using the service, his data has to be erased.
5. Data Quality: Users need to be able to update and modify their data; those operations, however, still require a level of information assurance to be provided by them in order to be performed.
6. Service User Access and Portability: Users have to be able to access their data promptly and whenever necessary, and to port them from an identity provider to the other without being locked in by proprietary formats.
7. Certification: Identity providers and service providers have to be certified in order to operate.
8. Dispute Resolution: An independent third party needs to be tasked with solving possible disputes arising between service users and identity providers.

[506] Privacy And Consumer Advisory Group (PCAG), 'Identity Assurance Principles V3.1' (2014).

[507] e.g. the encryption standard used by the identity provider.

9. Exceptional Circumstances: Any exception to the principles above needs to be sanctioned by law, transparent, accountable, and subject to scrutiny.

The following sections briefly outline the specifications and requirements that identity providers and service providers must implement when dealing with individuals and organizations aiming to use public online services.

Service provider requirements

Providing online public services attracts significant risk: several categories of potential attackers would benefit from unauthorized access to the service or its users' information. Online public services often deal with extremely sensitive and valuable information, and it is fundamental for the subjects running them to assess how to provide their services securely. As noted, "(w)hen considering the threats to a HMG Online Services, analysts should be aware that anyone or any organisation that has the capability and motivation to attack the service are highly likely to do so. Threats will seek to make use of lost, stolen, intercepted or hijacked identity information to gain unauthorised access to systems, information and services."[508]

The CESG and the Cabinet Office, in this regard, published a Good Practice Guide[509] aiming at setting the Requirements for Secure Delivery of Online Public Services (RSDOPS). Rather than listing particular protocols or security measures, the RSDOPS are "a response to the challenge of delivering online public services and sets out an approach to deriving, discussing, and agreeing security requirements for systems delivering public services electronically [...] The purpose of this document is to provide HMG departments and the wider public sector with a means to understand what is needed from a security perspective to support delivery of an online public service."[510] The Good Practice Guide focuses on end-to-end security, taking into account not only its technical aspects, but also the need to rely on secure business processes and stakeholder relations;[511] it does not substitute pre-existing standards and practices, but aims to inform and complement it.

The RSDOPS guide foresees the adoption of a six-step process to help service providers frame their security needs with a sufficient degree of clarity. The assessment's steps are as follows:

- Step 1: Identify & Describe the Security Challenge. The first step aims at identifying the security issues and concerns arising from the service's provision, after a descriptive but thorough examination of the business case around the model.
- Step 2: Identify Active Participants, i.e. the ones that will use, deliver, support, manage and regulate the service.

[508] CESG, Cabinet Office, 'Good Practice Guide No. 43 Requirements For A Secure Deliver Of Online Public Service' (Issue No 1.1, 2012), p. 23.

[509] CESG, Cabinet Office, Ibid.

[510] Ibid., p. 5.

[511] Ibid., p. 6.

- Step 3: Identify Stakeholders Expectations and Engagement. Different stakeholders have different security concerns with regards to the same service.
- Step 4: Identify Information Risks, through threat modeling and risk assessment. The good practice guide does not identify a specific methodology, even though some UK bodies are mandated to use the HMG Security Policy Framework (SPF) by policy or regulation. The risks assessed might be due to personnel, procedures, physical location or technical design, implementation and management.
- Step 5: Match the Information Risks to a Profile. The good practice guide exemplifies a set of security components[512] forming the RDOPS. A risk level has to be matched to each component, in order to form a granular risk profile.
- Step 6: Develop and Validate the Security Case. The final step builds upon the previous ones, framing the decisions and the proposals resulting from the precedent steps. The security case could contain, according to the guide, the following elements, and everything else the subject drafting the case deems relevant:
    - Overview of the service or transaction;
    - Description of any security challenges identified;
    - Summary of stakeholders, their concerns and expectations;
    - Summary of risk assessment activities and key findings;
    - Security profile recommended and supporting rationale;
    - Analysis of consequences of failure of specific security components.

Identity Proofing and Verification of an Individual

Identity Providers authenticate an individual's identification. In the UK there is no common set of attributes to be used for identification purposes. The CESG and Home Office's Good Practice Guide No. 45 on Identity Proofing and Verification of an Individual (GPG45), however, states the UK IPV verification requirements and allows interpretation in light of the relative international standards.[513]

The GPG45 describes the process to be followed for identity proofing purposes. Initially, the individual must declare his/her name, date of birth and address, known as Claimed Identity. The applicant will be then required to prove that the Claimed Identity exists, providing an Identity Evidence Package, either electronically or physically, depending on the particular requirements. The evidence provided is then subject to a validation and verification process, that checks whether it is genuine and valid and relating to that particular individual.

The Claimed Identity (*rectius*, its Activity History) will then be subject of background checks to determine whether there are signs of its existence in the real world. Moreover, the Claimed Identity will be crosschecked with specific databases to ensure that it is not a known fake or stolen

[512] e.g. authentication, information access, network protection, etc.

[513] e.g. ￼GPG 45, RSDOPS, STORK 2.0, 29115:2011, ISO 29003, NIST 800-63.

identity (Counter-Fraud Checks). The identity provider has to ensure that all the steps of the process are adequately completed. At the end of the process (whose steps do not have to be followed in a specific order) the individual will have an Assured Identity to be used as an authenticating credential.

The GPG45 foresees four different levels of identity proofing, which can be related to the levels foreseen by other Identity Proofing and Verification (IPV) standards. At Level 1 there is no specific requirement for the identity to be proven. The individual has provided an Identifier that can be used to confirm his identity and the Identifier has been checked to ensure that it is associated with the individual. A Level 2 Identity is a Claimed Identity with evidence that supports its existence and activity history. "The steps taken to determine that the identity relates to a real person and that the Applicant is owner of that identity might be offered in support of civil proceedings."[514] A Level 3 Identity is a Level 2 identity that physically identifies the person to whom it refers. "The steps taken to determine that the identity relates to a real person and that the Applicant is owner of that identity might be offered in support of criminal proceedings."[515] For a Level 4 Identity, the individual is also required to provide additional evidence; moreover, additional and specific processes, including the use of Biometrics, are foreseen.

As mentioned, the Claimed Identity provided by the applicants is subject to a verification process, whose checks are increasingly thorough according to the level of identification required. The Identity Evidence required in order to meet the requisites of the Identity Levels sketched above is evaluated according to the strength of its IPV elements.[516] In accordance with the Identity Level classification, there are five IPV elements. In order to be ranked in a specific category, the Identity Evidence provided by the individual must meet all the properties[517] required by the GPG45. The IPV elements enumerated by the GPG45 are:

1. IPV Element A – Strength of Identity Evidence;
2. IPV Element B – Outcome of the Validation of Identity Evidence;
3. IPV Element C – Outcome of Identity Verification;
4. IPV Element D – Outcome of Counter-Fraud Checks;
5. IPV Element E – Activity History of the Claimed Identity.

The IPV Operations Manual[518] provides detailed requirements and guidance on individuals' Identity Proofing and Verification.

[514] CESG, Cabinet Office, Ibid., 2014, p. 9.

[515] Ibid.

[516] Ibid., pp. 10 ss.

[517] e.g. to achieve an IPV Element C – Outcome of Identity Verification score of 3 an individual's Identity evidence would have to meet all the following properties: "*(t)he Applicant's ownership of the Claimed Identity has been confirmed by physical comparison using a photograph/image OR Biometric comparison of the Applicant to the strongest piece of Identity Evidence provided to support the Claimed Identity AND The Applicant's ownership of the Claimed Identity has been confirmed by a Static OR Dynamic Knowledge Based Verification*" – see *Ibid.*, p. 13.

[518] Cabinet Office and Government Digital Service, 'IPV Operations Manual v2.3.1 (redacted)' (2014).

Identity Proofing and Verification of an Organization

Individuals are not the only subjects that may benefit from using online public services: organizations often have the same need with regard to identity proofing, often needing to prove that a particular individual (the Responsible Officer) is responsible and accountable for the organization.

The CESG's Good Practice Guide No. 46 – Organisation Identity[519] (GPG46) provides a proofing process: after the verification of the identity of the individual applicant according to the process and standards foreseen in the GPG45, the (claiming) Responsible Officer shall provide an indication of the organisation he represents and the registered details of that organisation, if any. The checks that are to be performed in order to determine whether the individual applicant is the Responsible Officer for that particular organisation, if successful, determine also by inference that the applicant is a legal entity.

The GPG on RSDOPS (GPG43), mentioned above, specifies a number of security controls to be enacted to safely deliver an online public service. The GPG46 clarifies that "(a)t Level 0 for personal and corporate registration there is no requirement for assurance in a claimed identity. For Level 1 personal and corporate registration there is no need to disclose the real world identity of the individual or the organisation but registration using an asserted identity may be required to access the service, so no proofing of an asserted identity is carried out. If there is no need to know an individual's or an organisation's identity then it is simply not asked for." Hence, the requirements for Level 0 and Level 1 organisation identity proofing are not stated in GPG46. Level 2 and Level 3 of identity proofing testimony that the individual has declared that they are a Responsible Officer for the Organisation and that "(t)he level of assurance concerning the Applicant's identity and that they are a Responsible Officer for the Organisation, give sufficient confidence for it to be offered[520]", respectively, in support of civil or criminal proceedings.

There are three Organisation Proofing and Verification (OPV) Elements used to score from 0 to 4 an organisation's identity assurance level:

1. OPV Element A - Outcome of IPV of the Applicant's Identity[521]:
   0. IPV of the applicant *ex* GPG45 unsuccessful.
   1. The applicant has a Level 1 identity *ex* GPG45.
   2. The applicant has a Level 2 identity *ex* GPG45.
   3. The applicant has a Level 3 identity *ex* GPG45.
   4. The applicant has a Level 4 identity *ex* GPG45.
2. OPV Element B - Outcome of Verification of the Responsible Officer;
   0. Confirmation unsuccessful.
   1. No assurance of the applicant being a Responsible Officer was required.
   2. The applicant address is consistent with the organisation's one.

[519] CESG, Cabinet Office, 'Good Practice Guide No. 46 – Organisation Identity' (Issue No 1.0, 2013).

[520] Ibid., p. 7.

[521] Under the GPG45.

3. The Personal Details of the applicant match those of a registered Responsible Officer, or he has been confirmed by the organisation as their Responsible Officer.

3. OPV Element C - Outcome of Counter-Fraud Checks.
   0. The organisation is known or suspected not to be a legal one.
   1. No counter-fraud check performed.
   2. No confirmed evidence that the organisation is not a legal one through a reliable and independent source.
   3. No confirmed evidence that the organisation is not a legal one through a reliable and independent source and through a specified governmental source.

In order to reach an Identity Level of 2 or 3, an organisation has to score, respectively, 2 or 3 in each category.

Authentication credentials

Both Identity Providers and Service Providers need to use authentication credentials in order to link an individual or an organisation to a particular identity.

The Good Practice Guide No. 44 – Authentication and Credentials for use with HMG Online Services (GPG44)[522] foresees three levels of authentication for online public services, each of which mandates the use of authentication credential of a different strength. A Level 1 authentication demonstrates that the person requesting authentication is in possession of the credential for a legitimate account. Level 2 "provides sufficient confidence that the Credential is being used by the legitimate account holder, or with the explicit consent of the legitimate account holder, and might be offered in support of civil proceedings."[523] The authenticating credential must be bound to its owner and provide protection against theft. Level 3 authentications provide sufficient assurance that the credential is being used by the legitimate account holder or with his explicit consent, and might be offered in support of criminal proceedings. The credential must be bound to its owner and protect the transaction from attacks.

In order to qualify for a given Authentication Level, an authentication credential must reach the corresponding score in each of its elements. The Authentication Credential elements foreseen in the GPG44 are as follows:

1. AC Element A: Credential Type;
2. AC Element B: Quality of the Credential;
3. AC Element C: Management of the Credential;
4. AC Element D: Monitoring;
5. AC Element E: Authentication Service Characteristics;
6. AC Element F: Information Assurance Maturity of the Authentication Provider.

[522] CESG, Cabinet Office, 'Good Practice Guide No. 44 – Authentication and Credentials for use with HMG Online Services' (Issue No 2.0, 2014).

[523] Ibid., p. 4.

The guide details the requirements each element must fulfil to have a certain score. In order to reach a certain Authentication Level a credential must have a score equal to the level desired in all of its elements.

Transaction monitoring

Transaction Monitoring (TxM) is a particular monitoring technique that helps identity and service providers counter and prevent the risk of an electronic attack targeted toward online public services. It "comprises a complementary set of business processes which monitor authenticated online transactions in real time for signs of abnormal behaviour and provides appropriate alerts accordingly."[524] TxM does not stand alone, but is part of a broader procedure of deterrence, detection and response. TxM reviews ICT systems for suspicious behaviour and patterns in transaction data and aims to detect fraud. It is different from protective monitoring, which oversees ICT systems "by monitoring internal network connections and functions and flagging an alert when users or applications attempt to perform actions they are not supposed to, without necessarily knowing exactly what is causing the problem."[525]

The Good Practice Guide No. 53 – Transaction Monitoring for HMG Online Service Providers (GPG53), which sets out the requirements for TxM performance – assumes that "a Department's TxM service will be provided by a combination of Industry, central HMG service and Departmental service, and will draw on the services of Identity Providers (IdP) and Attribute Providers (AtP) in the process."[526] In certain circumstances, the performance of TxM is compulsory.

From a definitional perspective, TxM is a system that "compares all aspects of a transaction event against data and rule sets previously recorded as the normal profile for a particular user. Having already established what a normal transaction session should look like in terms of behaviour and various technical parameters, any element of the transaction event which falls outside the profile then triggers an alert which raises the risk score of the transaction."[527] A TxM system gathers data from many different levels, stages and parties of the transaction: such data could include, for instance, IP addresses, transactional content, timing, bank account details, identity and credential attributes, etc.

A TxM system can be regarded as fully operational when it is able to achieve the following tasks:

1. Capture of all transaction data;
2. Detection of abnormal behaviour;
3. Data storage and records management.

Overall, the "deterrence, detection and response" procedure in which TxM is integrated needs to allow public service providers or whoever executes it to perform the following activities:

[524] CESG, Cabinet Office, 'Good Practice Guide No. 53 – Transaction Monitoring for HMG Online Service Providers' (Issue No 1.0, 2013).
[525] Ibid., p. 7.
[526] Ibid., p. 1.
[527] Ibid., p. 6.

1. Transaction Event Monitoring;
2. Behavioral Monitoring;
3. Fraud and Error Monitoring;
4. Intelligence Feed;
5. Root Cause Analysis.

It is evident, on one hand, the degree of technical demand that the TxM would require, and on the other its potential to be strongly privacy–intrusive; hence, both a technical assessment and a privacy impact assessment are strongly suggested before its implementation.

Regulation of Incident Management

The basis of the Gov.UK Verify programme appears to be constituted mostly by private law instruments and good practice guides issued by public bodies; hence, in order to review how incidents are managed in the program's context, it is necessary to examine which incident management system each actor (e.g. IDPs, relying parties, etc.) composing the Gov.UK Verify program has in place in its own undertaking, which would exceed the scope of this report. Adherence to well-established international incident management standards, in particular to the ones addressing information security incidents[528] is arguably to be expected, given that an intentional breach of the confidentiality or of the integrity of the systems connected to the Gov.UK Verify could lead to distribution of users' relevant identifiers, which in turn could be instrumental in the commission of identity-related crimes.

While there seems to be no particular regulation aiming at the management of the incidents deriving from an attack targeted towards one of the components of the Gov.UK Verify program, the UK has developed a series of initiatives[529] that allow individuals to report identity crimes through a single dedicated contact point and provide information on the subject. Public and private initiatives aiming at providing information and raising awareness, such as informative websites, can play a crucial role in ensuring that consumers and businesses are informed on how to adequately address the event of an identity-related crime taking place, and on where and how to report it.

Regulation of Repression

Besides what is implied by the categorization of the Gov.UK Verify system as a critical infrastructure,[530] the UK's criminal legislation addresses the aftereffects of identity crimes.[531][532]

Identity Crimes Legislation

[528] e.g. ISO/IEC 27035:2011.

[529] Both of a public and of a private nature; e.g. ActionFraud (http://www.actionfraud.police.uk/), a portal through which any incident relating to fraud – identity crimes included – can be reported and that acts as a single point of contact in order to facilitate a follow-up. Another example is the activity carried on by Cifas (https://www.cifas.org.uk/), a non-profit organisation composed by a number of large companies that is dedicated to the prevention of fraud, identity and financial crimes.

[530] See also Chapter 4, on the protection of electricity-related CNIs in the UK.

[531] e.g. identity theft, identity fraud, and all the crimes committed as instrumental to other crimes revolving around an individual's identity or identification. There are several definitions that can be applied to "identity crime" and its related terms.

[532] See Neil Robinson et al, 'Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report' (RAND Europe 2011), p. 568.

There is no targeted legislation in the UK that explicitly criminalizes ID theft, ID fraud and other related crimes as specific offences, and therefore they are dealt with through the use of more general repressive provisions like the ones highlighted below. However, as mentioned, most cases of identity-related offences, such as operating a false identity on-line, unlawfully using another person's identity, deploying malware, phishing, and trafficking in personal data acquired illicitly, are effectively criminalized by the UK's legislation.

Section 2 of the Fraud Act,[533] 'Fraud by false representation,' criminalizes the activities of persons making a false representation, intending to make a gain for himself or another, or to cause loss to another or to expose another to a risk of loss. Any representation as to fact or law, be it express or implied) is deemed as false representation if it is untrue or misleading, and the person making it knows that it is so. Section 6 of the Fraud Act states that a person commits an offence if he has in his possession or under his control any article for use in the course of or in connection with any fraud – a provision that could be used to sanction the possession of software instrumental to the commission of an identity crime that exploits the Gov.UK Verify program. The following section, "Making or supplying articles for use in frauds", classifies as an offence the making, adaptation, supply or offer of any article while either knowing that it is designed or adapted for use in the course of or in connection with fraud, or intending it to be used to commit (or assist in the commission of) fraud. "Article", as section 8 specifies, includes any program or data held in electronic form. As identity crimes are often of an instrumental nature, section 11 sanctions obtaining services for oneself or another by a dishonest act, if those services are made available on the basis of a payment that has been, is being or will be made, and he obtains them without any payment having been made or without payment having been made in full, while knowing that they are or might be being made available on the basis of such a payment (or promise thereof), but he or she intends for that payment not to be made, or not be made in full.

Moreover, as has been noted,[534] the national legislation transposing the European data protection framework into national law, the UK Data Protection Act,[535] "could act in this respect as a convenient catch-all safety net for incidents with an otherwise unclear legal status".[536] Section 55 of the aforementioned act, 'Unlawful obtaining etc. of personal data,' criminalizes the conduct of whoever obtains or discloses personal data or the information contained in personal data, or procures their disclosure to another person.

Computer Misuse Act

The UK Computer Misuse Act 1990[537] (CMA) is specifically aimed at tackling the offences derived from the misuse of computers and networks; the CMA (as amended by the Police and Justice Act 2006) frames as punishable offences the unauthorised access to a system, the same access with

[533] Fraud Act 2006 (c. 35).
[534] See Robinson 2011, Ibid., p. XIII.
[535] Data Protection Act 1998 (c. 29).
[536] Robinson 2011, Ibid., p. XIII.
[537] Computer Misuse Act 1990 (c. 18).

the specific intent to commit or facilitate commission of further offences (e.g. identity theft) and the acts that intentionally, or unintentionally but recklessly, impair the operation of computer systems or networks. For a discussion on the CMA offences, we refer to the discussion of offences against the electricity provisioning CNI. Aside from its function in the repression of cyber attacks targeting the eID program as a critical infrastructure, the CMA also "provides for the manner in which identity crimes take place."[538]

5.3 Conclusion

This chapter examines how the identity infrastructure for citizen-government relations is organized in the selected countries. As in the previous chapters, the distributed responsibility and mutual dependency between actors is evident as they attempt to ensure the protection of individual privacy and citizen-specific data. There are four primary issues relevant to governance of these infrastructures: architecture and interoperability, use and citizen engagement, combating fraud and the role of legislative measures.

System architectures differ, with countries such as the UK opting toward more centralization ('hub') and other countries explicitly choosing for no centralized database. The latter is the case in Germany, but is perhaps most evident in Canada, where the distributed responsibility for identity among federal, provincial and territorial governments has led to a diversity of e-identity infrastructure initiatives that now need to be made interoperable. (A Joint Council of Federal, Provincial and Territorial Governments is working on a 'Pan-Canadian Identity Trust Framework'.)

Trust in systems is important not only between the actors working to protect the infrastructures, but also from the end-users, i.e. the citizens. From a privacy and data protection perspective, the German eID infrastructure seems to be exemplary for taking the right approach to infrastructure protection. The role of the need-to-know principle in preventing the misuse of personal data and gaining transparency, the possibility to limit data transfers within the scope of the European Data Protection Directive and the possibility to validate the identity of the interaction partner have been especially highlighted.[539] However, despite the positive evaluation, the eID infrastructure has not been used as widely as initially expected. As of 2014, only about one third of all the ID cards had the function activated.[540] This is generally attributed to poor marketing, lack of perceived value and the low number of service providers that can access the card,[541] but could also be attributed to the relative novelty of the system, whereby some use issues could eventually be resolved over time. In the move toward such systems, the Estonian case example in this chapter, which outlines how the state actively engages and informs its citizens, demonstrates the importance of transparent communication strategies when implementing such infrastructures.

[538] David S Wall., 'Future Identities: Changing identities in the UK – the next 10 years' (DR 19: Identity Related Crime in the UK, Durham University, 2013), p. 18.

[539] Hornung and Roßnagel 2010, p. 155.

[540] C Hoffmann, 'Warum die eID-Funktion des neuen Personalausweis (noch) keinen Erfolg hat' (2014) Government2020.de blog, available at: http://www.government2020.de/blog/?p=1420.

[541] Rosner 2014, p. 184.

Once use is secured, not only protecting individual data by identifying weaknesses in the system, but also combating fraudulent use becomes an important aspect of governance. This was especially relevant in the Dutch case, where much discretion is left to individual actors. In this case, customers are free to decide how to use DigiD in their application domain, e.g. they choose the security level, whereby security may be balanced against other interests such as ease of use, which was apparent in the tax fraud case. Recent research[542] claims that the Gov.UK Verify program "suffer from serious privacy and security shortcomings, fail to comply with privacy-preserving guidelines they are meant to follow, and may actually degrade user privacy."[543] The main area of concern regards the hub that links users' interactions across services, is able to see citizens' personal data and, if compromised, would allow a malicious insider to impersonate a user. As a consequence, and considering its forensic capabilities, the hub has the potential to be used for mass surveillance purposes.[544] Despite the principles set by the PCAG, the CESG guidelines and best practices, and the decentralized architecture of the Gov.UK Verify system, the UK's eID framework still raises certain privacy and security concerns. Such problems were not encountered during the quick scans of the other studies (even when asked about during the validation interviews), but Germany, for example, continues tests to find these types of systemic vulnerabilities.

The interest of security, the interdependence among actors and the discretion attributed to some actors require a security-oriented mentality among the actors. Such mentality cannot or hardly be enforced legally. Other instruments, such as information provision and EDP audits, therefore play an important role. Nonetheless, the high degree of mutual dependence between the different actors, in both the vertical chain (Government actor + Private parties/service providers + Customer + End User) and the horizontal chain (customers + other customers), provides strong legitimization for regulation. Omissions by one party often have implications for other parties, which means that there should not only be a clear distribution of responsibilities but also specific mechanisms in place to ensure that these responsibilities are taken seriously. Although the operational security of most of the systems discussed here must still be shaped, there are other initiatives reinforcing cybersecurity in this domain, such as the comprehensive criminalisation of identity theft in Canada and broader initiatives that have particular relevance for cybersecurity in relation to identity. In the Netherlands, actors currently rely on a web of contracts; in case of disputes, actors like the Ministry and Logius rely on civil remedies, which may be slower in application than public instruments. Also the Estonian case shows the important role of key legislative decisions in paving the way for actors to create a securely functioning identity infrastructure for both online and offline transactions. Specifically, giving online exchanges equal status and protection is a key element of that case.

[542] Luís T.A.N Brandão, Nicolas Christin, and George Danezis, 'Toward Mending Two Nation-Scale Brokered Identification Systems', (Proceedings on Privacy Enhancing Technologies, 2015.2, 2015), pp. 135-155.
[543] Ibid.
[544] Ibid.

The identity infrastructures reviewed in this quick scan are quite new, with most still being developed. They exemplify both the trial-and-error nature of experimentalist governance and the social transition identified in Chapter 2 under the section on risk governance. There is indeed an expanding arena of actors, shifts between public/private relations and tensions between processes of centralization and decentralization. Rather than restricting the capacity of traditional authority as is stated in these governance theories, however, these developments (and the concretization of approaches in specific technological architectures) highlight areas where traditional governance strategies such as regulation fall short, e.g. in creating a security-oriented mentality, but at the same time also legitimize the need for more clarity of roles which can be offered through regulatory (legislative) measures that clarify roles, rather than leaving decisions to the discretion of multiple actors.

6. Discussion and Conclusion

This report provides a quick scan of the landscape of cybersecurity governance in five countries. In order to make a feasible overview, we selected three diverse cases: botnet mitigation, vital infrastructure protection, and identity infrastructure in government-citizen relationships. These cases were selected because they are diverse (which provides for a richer analysis than only examining cases that lie close to the core of cybersecurity), cover the main aspects of cybersecurity (confidentiality, availability and integrity), cover different domains in which government classically plays an important role (law enforcement, national security, and service delivery) and involve different levels of private-actor involvement. The cases thus shed light on the multifaceted nature of cybersecurity and reveal various shifts in forms of governance. In this chapter, we first briefly summarize the key findings in answer to the research questions and then revisit the primary concepts discussed in Chapter 2. In revisiting the primary concepts, we introduce two critical views presented in the literature, in order to further nuance the view of cybersecurity governance in policy and practice. We then outline six lessons learned/points for further consideration.

6.1 What is cybersecurity?

Cybersecurity denotes the process and result of making cyberspace secure, where cyberspace refers to the space constituted by information, ICT, networks, and (ICT-based) infrastructures. Although cyberspace is based on technological components, it is not identical to physical space, i.e., the technological layer itself; it also includes the abstract space of digital, interconnected human and organisational activities. The security of this space consists of being free from threats to the confidentiality, integrity, or availability of the computers, networks, and information that together make up this space. Cyberspace itself, and the human and organisational activities using this space ideally should not suffer from malfunctions in the infrastructure or any of its components, or from attacks on the infrastructure, its components, or the information processed using the infrastructure or its components. In short, cybersecurity can be defined as the proactive and reactive processes working toward the ideal of being free from threats to the confidentiality, integrity, or availability of the computers, networks, and information that form part of, and together constitute, cyberspace—the conceptual space that affords digitised and networked human and organisational activities.

Given the increasing multitude of players interacting in the cybersecurity landscape, there is a need to cooperate and coordinate in order to prevent threats to this infrastructure and its component parts, as well as a need to deal with incidents when they occur. Cybersecurity governance can thus be defined as the approaches used by multiple stakeholders to identify, frame and coordinate proactive and reactive responses to potential threats to the confidentiality, integrity, or availability of the computers, networks, and information that together constitute cyberspace (the conceptual space that affords digitised and networked human and organisational activities). This includes not only short-term and concrete approaches to address known threats, but particularly also the development and implementation of structures and processes to reduce uncertainty and to enable to respond to threats from unanticipated events over the longer term.

6.2 How are the responsibilities for cybersecurity distributed among relevant actors?

The three case studies, taken together, show a progression in understanding of what constitutes cybersecurity and how to ensure that the relevant structures are in place. In all countries a number of policy documents and strategic action plans have been produced by various federal agencies, police authorities and/or key interest groups, highlighting increased attention for the need to protect information infrastructures at various levels. An examination of UK and German policy documents, for example, shows the increasing specificity of the language used to refer to what constitutes a given infrastructure, the nature of possible threats to that infrastructure and the subsequent social sectors that will feel the effects of those threats. At the same time, such documents reveal the high degree of polycentric governance in each country and in relation to each case, which can lead to confusion regarding who is responsible in the case of a major incident (seen, for example, in the case of Germany's vital infrastructures) and makes it somewhat difficult to compare between national-level approaches.

Interestingly, which national agency (department or ministry) is responsible for the primary agenda-setting and coordination efforts varies per country (and, to a certain degree, per case). Whereas in the Netherlands, the Ministry of Security and Justice is the leading authority, in other countries, such as Estonia, it is the Ministry of Economic Affairs and Communications (although the Ministry of Justice also plays a role). Specifically, and perhaps not unsurprisingly, with regard to vital infrastructure protection, there is a greater role for departments that handle Foreign Affairs and thus also for policing forces and the military (as in Canada and Germany). Increasingly, there also seems to be recognition that the nature of the problem is so large that it is insufficient to designate one lead agency, whereby there have been mergers between two or more previously distinct bodies, as in the UK, or new cooperative arrangements formalized between agencies responsible for different sectors. What is less clear is the degree to which each of these agencies has an identified coordinator status with a given final decision-making authority and where this coordination role is better described as one of providing guidance, promoting best practices and engaging in activities to facilitate collaboration with and between other actors.

The case of botnets discussed in Chapter 3 showed that, in addition to the responsible government agency, all of the countries included in this quick scan have at least a national CERT in place, with the mandate to oversee the dissemination of threats on national territory. While the procedures followed by CERTs are to a large extent harmonised, the practical value of their operations in regard to botnets varies. Moreover, because CERTs work within specified circles of trust, they share relevant information with one another that may not be disclosed to a larger audience, making it nearly impossible to evaluate the impact and the influence of national CERTs countering botnets beyond what stated online. Nonetheless, in countries such as the UK, parties are increasingly encouraged to develop their own CERTs, which could potentially lead to less information sharing (and thus, partial knowledge of threats), without any demonstrated additional benefit.

Chapter 3 also showed the importance of multi-stakeholder mitigation efforts at the international level. Despite national variations in approaches to botnet mitigation, all countries have demonstrated participation in international cooperative efforts against botnets. Despite the widening arena of actors and concordant shifts in the division of responsibilities, at the moment that coordinated action was necessary to take down a botnet in these situations, the C&C function of the government and police became evident. Initiatives supported by public authorities were easier to identify than sectoral and inter-sectoral efforts, for example the Virtual Situation Room run by the Estonian CERT. A large part of the international cooperation activities against botnets revealed a connection with EUROPOL (EC3) and the FBI efforts in fighting botnets, demonstrating the important role played by both institutions and a significant level of international cooperation.

Whereas the distribution of authority across sectors and many levels of government could potentially be problematic from a governance perspective, especially in countries with a division of power between federal and state or provincial domains, Chapter 4 showed that this is perhaps not as great a problem as one might initially expect. The example of the energy sector clearly shows that critical infrastructure protection at the national level is a key issue that is increasingly seen as a joint task of society at large – suggesting more distribution of responsibilities across sectors, levels of government and types of individual and corporate actors. This was evident in German calls for more coordinated action supported by all players – government, business and industry and the general public – as well as in the role afforded to individual citizen vigilance in policy documents on the governance of Canadian vital infrastructure.

One issue that became evident in Chapter 4 (and 5) was the increasing importance of the role of private sector parties, especially in countries where liberalization of markets has led to unbundling of functions and thereby a more distributed governance network. The economic aspect was mentioned as a point of contention in the Canadian case, and in the German case the issue of private actors currently only participating in collaborative and cooperative partnerships on a voluntary basis raises concerns about the actual effectiveness of such structures in preventing serious infrastructure threats. This is an important point to consider because it demonstrates how the choice for new measures (and thus who is responsible for them) touches upon the general interest and therefore legitimises certain government involvement. This is perhaps one reason that economic agencies have a more prominent role in some of the countries examined in this study.

Chapter 5 revealed a myriad of approaches to identity governance in the internet era. The role of private sector parties was also prominent here, largely in settling contracts with government for the provision of various services and products necessary to a secure and functioning infrastructure for individual identification, authentication and authorization. Estonia and Germany further demonstrate how industry can be instrumental in the adoption (as in the case of Estonia) or non-adoption (as in the case of Germany) of policies and practices that ensure the protection of identity-related transactions in a digital environment. The Canadian case showed one of the drawbacks of having so many different players active in this field: after implementing systems, ensuring the interoperability between (geographically) distinct systems while still effectively protecting the data they are transmitting poses a new governance challenge. Especially the incidents related to identity protection mentioned in the Dutch case highlight the importance of having systems in place that allow for quick detection of malfunction and criminal activities, which further points to the relevance of not only technical interoperability, but also cooperation between key players.

Finally, with regard to the distribution of responsibilities, examining how the different countries deal with the specific cybersecurity challenges presented by each case type reveals the importance of considering other aspects of governance than just the mutual interdependence between public and private actors. The cases show that counteracting the security threats posed to the various infrastructures is rarely a merely technical solution; rather, communication is a key part of governance processes, be it informing the affected parties after the fact or raising public awareness as part of preventive strategies. Moreover, they all point to the need for reflexivity and iterative learning in governance processes, as discussed in Chapter 2, which is especially critical given the dynamic nature of the cybersecurity landscape and the fact that actors cannot always foresee and oversee all the possible threats and their consequences.

6.3 How are the responsibilities for cybersecurity regulated by law?

In examining the legal side of cybersecurity governance, we discussed the regulatory frameworks for prevention, incident management and repression of threats to cybersecurity. Although the three cases cannot be generalised or even comprehensively summarised, given their specificity and complexity, we can sketch a preliminary picture that emerges from the cases.

Regulation of prevention often takes the form of sectoral laws, possibly combined with lower regulations, stipulating requirements for risk assessment and risk management in a certain sector. There is some regional harmonization, such as the proposed EU Directive on network and information security (NIS), but we encountered few international regulatory frameworks here, except some references to international security standards such as the ISO norm for information security. Preventive regulation is, unsurprisingly, most prominently seen in the field of critical infrastructures, where it particularly makes sense to invest in prevention of high-risk threats; besides critical infrastructures, it can also be observed in regulating specific elements of cyberspace, such as protection of personal data or of telecommunications, where security requirements aim to provide a basic level of protection against generic cybersecurity threats. Besides legislation, we see prevention also being approached through information sharing, between and among various public and private stakeholders, which sometimes but not always seems to be underpinned by some form of regulation, such as contracts or another form of agreement between parties. One important aspect of prevention for which we encountered only a few examples (although this may well be due to the quick scan character of the report, which necessarily relies more on law in the books than law in action), is enforcement of preventive measures. One interesting example of a preventive regulatory framework that includes significant measures of oversight is the German Energy Industry Act. It is a question for further research to what extent regulatory frameworks also provide for sufficient measures to ensure compliance with preventive standards and procedures, including oversight.

Regulation of incident management seems less developed than regulation of prevention or repression. The primary focus of regulators is security breach notification, to ensure that cybersecurity threats are timely known at the appropriate level(s) where adequate incident response can be coordinated and performed. It is also assumed that mandatory security breach notification will have some preventive effect, since organisations will want to prevent the burden (and possible reputation damage) of having to report breaches in their cybersecurity. Regulators seem to be struggling with security breach notification regulation: many measures are still being developed, both at the supranational and at the national levels, and we see a fragmented approach with different, and possibly overlapping, measures being proposed or adopted. Most prominent is the security breach notification requirement in the EU NIS Directive, but there are also notification requirements in personal data and telecommunications regulation. Moreover, it remains to be seen to what extent the NIS Directive will be implemented in the same way in different member states; the developments in Germany with the IT Security Act, for example, seems suggestive of a sectoral and piecemeal approach, possibly leading to different forms of notification requirements or procedures.

The fact that notification requirements apply in different sectors and for different aspects of cyberspace (data, communications infrastructure, type of service), which often have different authorities as the addressee of notifications, implies that a comprehensive overview of cybersecurity threats will not be achieved, unless further efforts are taken to streamline or coordinate the different types of notifications. Here we see the complexity of cybersecurity governance in action: cyberthreats can be approached from different angles (threats involving the technological (communications) infrastructure, the data flowing over this infrastructure, and the meaning of these data (the informational content) in different application contexts), and since these angles are often associated with different responsible actors, it is difficult to have a comprehensive approach to cybersecurity, even for something as relatively straightforward as notifying a breach of security. It may also be telling that the primary regulatory effort encountered in the cases is security breach notification; other elements of incident response are (even) less clearly or visibly regulated.

This contrasts with regulation of repression, where we find considerable similarities and a consistent effort in regulatory approaches in the different countries. This is particularly the case in substantive law, which is harmonised to a considerable degree through the Cybercrime Convention. With the recent accession of Canada, all countries we studied have ratified and implemented the Convention, which is a sign of its global importance. The Convention and national implementations provide a minimum level of criminalisation of cyberattacks, and since the types of attacks are defined in a generic and relatively technology-neutral way (as unlawful access to, interception of or interference with networks, computers or data), this provides a good basis to prosecute perpetrators of cyber-attacks, regardless of the particular modus operandi or the type of computer or data involved.

The Convention does have limitations, however. One is that it does not mention sanction levels; EU Directive 2013/40/EU provides a more forcible model in this respect, as it prescribes minimum levels of criminal sanctions, and also includes particular aggravating circumstances (and higher sanctions) for use of botnets or attacks against critical infrastructures. A Guidance Note to the Cybercrime Convention on sanctions might be helpful in this regard. Another limitation, at least from the perspective of cybersecurity, is that repression through criminal law is generally only possible for intentional attacks, not for negligence or accidents. Repressive measures against those who are sloppy with cybersecurity are also important, but this should be done, for example, by enforcing professional standards through tort law, rather than criminal law.[545] Moreover, substantive criminal law only works if it is enforced, so procedural law is equally important. Here we see less harmonisation and more differences between countries, even though the Cybercrime Convention also provides minimum standards for investigation powers. The discussions in Canada on lawful interception and in the Netherlands on remote access to computers by police show that state powers to investigate cyberattacks are a sensitive issue, all the more so in a post-Snowden context where the issue of government surveillance leads to wider societal debates. These sensitivities are difficult to resolve, and will require fine-tuned, national approaches rather than international guidelines. Since cyberinvestigation is – by its nature – easily cross-border investigation, this is a particularly challenging area in cybersecurity governance.

Taking the above into consideration, we can conclude that the regulatory framework of cybersecurity has certain international elements, e.g., in cybercrime legislation and technical standards, but is largely undertaken at the national (and sometimes sub-national, in federated countries) level. Supranational regulation is visible in the EU, but rather limited to certain aspects of cybersecurity, such as critical infrastructures and telecommunications regulation. This is not to say that regulatory frameworks are necessarily fragmented at the supranational level – e.g., policy learning or legal transplants might take place, which we cannot determine on the basis of a quick scan – but at least it is clear that a comprehensive global regulatory effort to cybersecurity is not visible in the cases we studied. A similar observation can be made at the national level: most cybersecurity regulation is relatively specific, covering a particular aspect of cyberspace or of security, or cybersecurity in a particular context. Comprehensive regulatory frameworks are rare – understandably so, given the complexity of cybersecurity as we highlighted in Chapter 2. However, the UK Civil Contingencies Act 2004 provides an interesting example of a more comprehensive

[545] See Tjong Tjin Tai et al. 2015 for an elaborate discussion of this point.

approach, constituting the UK's general framework for local and national emergency planning, management and response, excepting only defence issues.

Finally, it is clear that law is not the only regulatory instrument in cybersecurity, although it plays an important role in all areas, as a general framework or as backstop regulation for situations that cannot be dealt with by private regulation alone. Legal frameworks are supplemented by, or – more often – expanded and detailed in, lower forms of regulation, such as administrative codes or (technical) standards, which may be explicitly made mandatory through a law as a minimum level of security or implicitly incorporated through a reference to open norms. Thus, cybersecurity regulation is often layered regulation, with more general legislative legal norms and more concrete lower-level norms. In several cases, soft law can also be observed that is not necessarily part of an overarching legislative framework; stakeholders make agreements with each other or develop guidelines or principles that serve as reference points for a sector or a certain type of organisation or professional. Particularly in the case of identification infrastructures, we encountered relatively few general legal frameworks, and more regulation through soft law, in particular also through contracts between public and private parties, where Terms & Conditions play an additional role in the governance of behaviour (in particular for the contracted private parties and the businesses or end-users with whom they engage). Here we can see the role of the state shift from being (only or largely) a public-policy maker and coordinator of society to being (also) one stakeholder among many with an interest in governance.

6.4 Putting cybersecurity governance into perspective

The form of a quickscan report does not allow us to elaborate and embed the findings of the use cases in a further theoretical reflection of cybersecurity governance. However, with a view to drawing lessons from the use cases, it is useful at this point to take one step back and to briefly discuss how the landscape of cybersecurity governance, as visible in the use cases, has come about, and how some of the challenges emerging from these could generally be approached by the stakeholders in governance.

Cybersecurity is a term that is used in certain ways, which is captured by the notion of *securitisation* – a discursive practice with a particular rhetorical structure, framing political debates in terms of the need for providing (one or another form of) security. The term cybersecurity, being a part of the political security discourse, was politicised by policy makers very early on in its development, and cybersecurity can be seen as 'a classic case of securitization'.[546] In the US, for example, cybersecurity was first presented as a matter that requires the attention of state actors because it cannot be solved by market forces.[547] As concern increased, policy-makers also represented it as a challenge requiring the urgent attention of the national security apparatus. Concern about security framed the issue either as a special kind of politics or as above politics:

[546] Broeders 2014, p. 8.
[547] Hansen and Nissenbaum 2009.

with securitisation, an issue is no longer debated as a political question, but dealt with at an accelerated pace and in ways that may come to violate normal legal and social rules.[548]

A key element of securitising discourse is creating a sense of urgency: arguing that if action is not undertaken then serious incidents will materialize in the near future. This is a specific rhetorical strategy to legitimize a proposed governance solution for a given situation, but at the same time offers opportunities to assess actual damage in attack situations (rather than only modelling the possibilities). Particularly events such as *Stuxnet* in 2010 or the cyberattacks on Estonia in 2007 catapulted cybersecurity from the expert level to the diplomatic and foreign policy realm, so that cybersecurity became an issue for diplomats, foreign policy analysts, the intelligence community and the military.[549] Cyber-risks – especially in their most extreme form (in the sense of cyberterrorism etc.) – fit the risk profile of so-called 'dread risks,' which are perceived as catastrophic, fatal, unknown and basically uncontrollable. That is why they cause disproportionate fear despite low probability, which translates into pressure for regulatory action of all sorts and the willingness to bear high costs for uncertain benefits.[550] A good example of the 'remarkable mobilization of securitizing prose' is an incident in the late 1990s, when two young hackers, Pryce and Bevan, were described in US Congress hearings as, "possibly the single biggest threat to world peace since Adolf Hitler."[551] The case against Bevan was dropped, and Pryce was fined the equivalent of £1200. Bevan said: "Looking back, I now believe that my case was not about hacking, but an exercise in propaganda."[552]

One risk of securitisation discourse is that it can lead to 'hypersecuritization', meaning an expansion of securitisation beyond what is considered to be a 'normal' level of threats and dangers, by defining ''a tendency both to exaggerate threats and to resort to excessive countermeasures."[553] Another characteristic of the securitisation discourse is 'technification' – it is dominated by technical and expert discourse with a strong emphasis on the hypothetical. These are both known strategies for dealing with the complexity and uncertainty that accompanies a risk such as cyberattacks, and although they might seem to make the cybersecurity landscape more manageable, it can mask the fact that the landscape is, in actuality, not overseen by policy-makers. The knowledge required to master the field is daunting and often not available to the broader public and as in most academic fields, computer scientists have disagreed on the likelihood of different forms of attacks. Moreover, since part of the field is cloaked in military or business secrecy, "much is withheld or simply not known, and estimates of damage strategically either wildly exaggerated or understated."[554]

[548] Hansen and Nissenbaum 2009.
[549] Dunn Cavelty 2012.
[550] Ibid.
[551] David S Wall, *Cybercrime* (Polity Press 2007), p. 24, referring to R Power, *Tangled Web. Tales of Digital Crime from the Shadows of Cyberspace* (Que 2000), Chapter 6 and M Bevan, 'Confessions of a hacker' (Sunday Business Post Online, 1 April 2001), available at http://www.kujimedia.com/confessions-of-a-hacker-by-mathew-bevan/.
[552] Wall 2007, p. 24, referring to Power 2000 and Bevan 2001.
[553] Barry Buzan, *The United States and the Great Powers: World Politics in the Twenty-First Century* (Polity Press 2004), p. 172.
[554] Nissenbaum 2005, p. 72.

Technifications thus support hypersecuritisations, whereby they play a crucial role in legitimating cyber-securitisations. With the shift from computer security to cybersecurity as described in Chapter 2, the original technical discourse has become linked to the securitizing discourse “developed in the specialized arena of national security”,[555] whereby cybersecurity can be seen as a development of computer security evolving into network and infrastructure security combined with a process of securitisation.

Closely related to, yet conceptually distinct from, the process of securitisation is a process of *criminalisation* – or perhaps, rather, of ‘*crimification*’ – that is visible in policy in the past decades. This is the phenomenon of using criminal law as a key instrument to address societal problems, rather than as a last resort (which criminal law traditionally has been) that is only used if other approaches (less invasive of fundamental rights and liberties) turn out insufficient. In the ‘crime society’, issues are often examined through the lens of criminal law: should we not criminalise new forms of behaviour that are causing problems, and should we not give the police more investigation powers?[556] As a result, many activities are criminalised in the early stages before harm is actually done, as is visible in, e.g., criminalisation of preparation and facilitation of (cyber)terrorism, and of misuse of devices (art. 6 Cybercrime Convention), i.e., the creation, trade, or possession of passwords, software or hardware if this occurs with intent to commit a cybercrime. From a governance perspective, the process of crimification is not necessarily wrong, but it raises questions of subsidiarity (is a new measure really necessary, given existing possibilities or alternative approaches, including non-criminal law or soft law?) and the cumulative effect of disparately adopted measures (e.g., the combination of measures may have side-effects not foreseen when measures are decided upon). Moreover, it raises questions of the organisation of legal protection, given that most checks and balances in criminal law are focused on the criminal trial, which does not protect citizens from the many risk-based and pre-emptive interventions (which do not lead to a trial in court) that are becoming an intrinsic part of cybercrime, and hence also of cybersecurity governance.[557]

Being aware of these issues helps position the discourse and policy-making efforts in the field of cybersecurity. In critical literature on cybersecurity governance, efforts are made to distinguish approaches based on inflated threat scenarios from realistic approaches to cybersecurity. Two concepts from this literature that can possibly help avoid tendencies toward hypersecuritisation, and thus are relevant to present here as ways that can help achieve a balanced and realistic approach to cybersecurity governance, are the “cybersecurity ladder” and “balanced risk approach”.

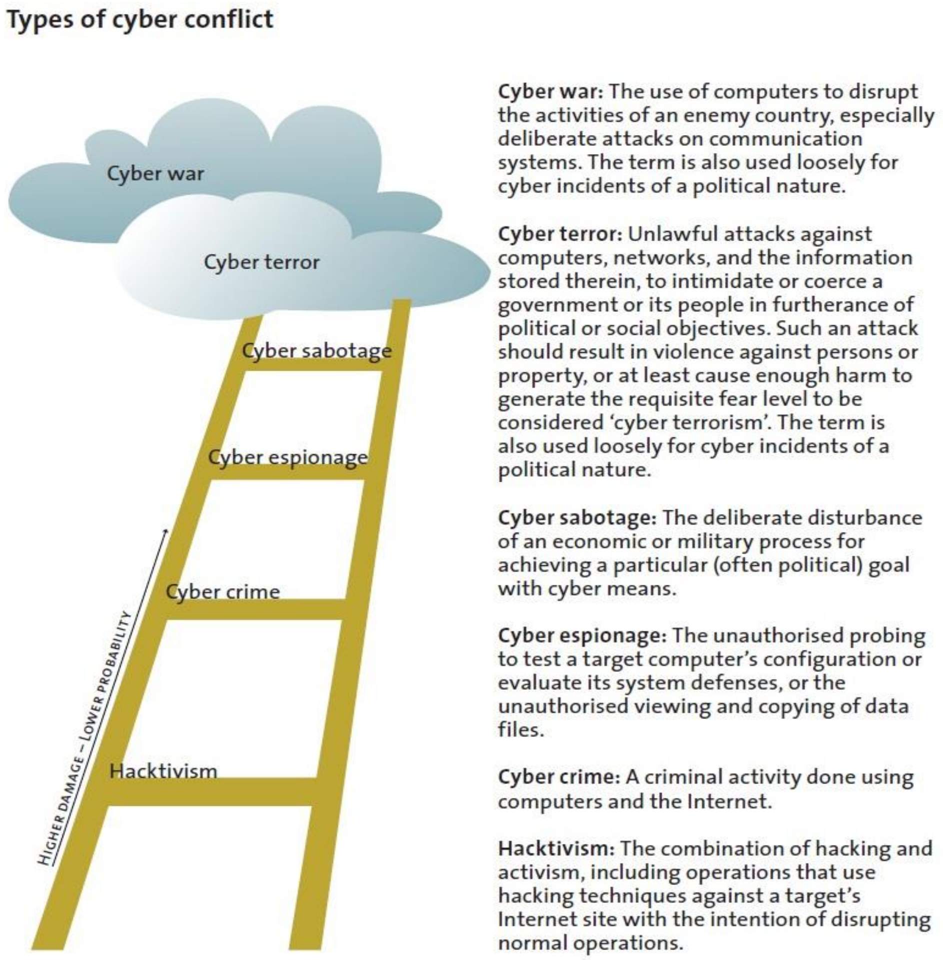
[555] Nissenbaum 2005, p. 65.

[556] B.J. Koops, ‘Technology and the Crime Society: Rethinking Legal Protection’ (2009) 1 *Law, Innovation and Technology* (1) 93-124.

[557] Ibid., p. 118-120.

6.4.1 The cybersecurity ladder

One effort to provide a nuanced view on cybersecurity governance is the development of the cybersecurity ladder. The idea behind this ladder is based on the *likelihood* of a cyberattack and the damage it *might* involve. Cyberincidents are continually causing minor and only occasionally major inconveniences (e.g., loss of intellectual property or other proprietary data, maintenance and repair, lost revenue and increased security costs).[558] In the entire history of computer networks, there are only a few examples of cyberattacks that resulted in actual physical violence against persons,[559] and only few had a substantial effect on property so far, although with the rise of the Internet of Things this may change in the future. Cyberattacks have not yet caused serious long-term disruptions – they are mainly risks that can be dealt with by individual entities using standard information security measures and their overall costs remain low in comparison to other risk categories such as financial risks.[560]



Types of cyber conflict

Cyber war: The use of computers to disrupt the activities of an enemy country, especially deliberate attacks on communication systems. The term is also used loosely for cyber incidents of a political nature.

Cyber terror: Unlawful attacks against computers, networks, and the information stored therein, to intimidate or coerce a government or its people in furtherance of political or social objectives. Such an attack should result in violence against persons or property, or at least cause enough harm to generate the requisite fear level to be considered 'cyber terrorism'. The term is also used loosely for cyber incidents of a political nature.

Cyber sabotage: The deliberate disturbance of an economic or military process for achieving a particular (often political) goal with cyber means.

Cyber espionage: The unauthorised probing to test a target computer's configuration or evaluate its system defenses, or the unauthorised viewing and copying of data files.

Cyber crime: A criminal activity done using computers and the Internet.

Hacktivism: The combination of hacking and activism, including operations that use hacking techniques against a target's Internet site with the intention of disrupting normal operations.

Types of cyber conflict, as identified by Dunn Cavelty (2012), p. 116.

[558] Dunn Cavelty 2012.

[559] Perhaps the attack by MacDonald's employees on Steve Mann wearing a skull-mounted camera in a *McDonald's* in Paris in 2012 could be counted as one.

[560] Dunn Cavelty 2012.

Thinking about and planning for worst-case scenarios is of course a legitimate task of the national security apparatus, however, based on probable risk and damage incurred, certain types of cyberattacks that are sometimes included in the definition of cybersecurity, such as cyberwarfare or cyberterrorism, should not receive too much attention at the expense of more plausible cyberproblems. Using too many resources for high-impact, low-probability events – therefore having fewer resources left for the low to middle impact and high probability events – does not make sense, neither politically, strategically, nor from a cost-benefit perspective. The focus should be on types of attacks that are more likely and even common, such as cybercrime, cyberespionage and attacks on critical infrastructures.

6.4.2 A balanced risk approach to cybersecurity

In keeping with the idea of risk governance mentioned in Chapter 2, another way of conceptualizing cybersecurity is through risk analysis. As mentioned above, in the last couple of years the definition of cybersecurity, particularly in NCSs, has been expanding to also include cyberterrorism and cyberwarfare. Moreover, after the attacks in the US on September 11, 2001, attacks affecting critical infrastructures have been labelled terrorist attacks and critical infrastructures have emerged as an increasing priority in counter-terrorism activities.[561] Although this report is not advocating widening the definition of cybersecurity to include cyberwarfare or cyberterrorism (which would include critical infrastructures), at least not as high priority cybersecurity goals, a risk analysis approach, also advocated as a counterterrorism policy,[562] to decision-making in regard to cybersecurity is proposed.

The risk analysis approach to decision-making states that allowing emotion to overwhelm sensible analysis is understandable and common among average citizens, however, it is inappropriate, irresponsible and even dangerous for the officials trying to keep them safe.[563] Taking the risk analysis approach means that four issues are applied to the threats presented by cybersecurity as it is defined: (1) the cost per saved life; (2) acceptable risk; (3) cost-benefit analysis; and (4) risk communication. Graver cybersecurity threats, e.g. terrorism, evoke extraordinary fear and anxiety in people. Since there the public places pressure upon decision-makers to act (and sometimes overreact), decision-makers are often also overly fearful about negative reaction to any relaxations of security measures that fail to be cost-effective and are otherwise seen as appropriate response with regard to possible consequences.[564] There are, thus, serious psychological and political aspects of risk perception and electoral and lobbyist pressure. In spite of this, it is has been found that regulators and administrators are generally unwilling to spend more than a certain amount (changing with time) to save a human life; if the investment

[561] European Commission in a communication on critical infrastucture protection in 2004 – the EC lists the protection of infrastructurs alongside the protection of borders and citizens, in Claudia Aradau, 'Security that matters: Critical infrastructure and objects of protection' (Department of Politics and International Studies, The Open University, Milton Keynes, UK 2010), p. 491.

[562] John Mueller and Mark G Stewart, 'Responsible counterterrorism policy' (2014) 755 CATO Institute Policy Analysis. Available at: http://object.cato.org/sites/cato.org/files/pubs/pdf/pa755.pdf

[563] Mueller and Stewart 2014, p.1.

[564] Mueller and Stewart 2014, pp. 1-2.

would exceed this ceiling, they would prefer to spend funds on measures that save lives at a lower cost.[565] This is the *cost per saved life* part of the risk analysis approach.

Another way to approach the issue is by looking at what individuals consider to be *acceptable risk*, i.e. compare annual fatality rates caused by cybersecurity attacks with those caused by other hazards. The central issue here is whether the likelihood of being killed by the threat is unacceptably high or is low enough to be acceptable: how safe is safe enough? To take an extreme example from the CATO paper: every year a few thousand people in the US die in falls from buildings that are more than one story high. Those lives could be saved by closing off all buildings at the ground floor – to reject such a policy would be to say tall buildings are worth that cost in lives. Indeed, as a society, we regularly and inescapably adopt policies where human lives are part of the price.[566] However, if this approach only looks at fatality rates then it would hardly be useful for cybersecurity threat analysis, since not many cyberattacks in fact result in death or serious physical injury. The 'injury' of cyberattacks is usually of a different kind – it is in distributed financial loss, loss of political or trade secrets, loss of privacy (or identity), annoyance and loss of capacity to conduct our lives in all aspects as we are used to.[567] The consequence in the 'acceptable risk' part of the risk analysis should, thus, be defined differently – threats that fall in the unacceptable range should be determined and these should then generally command the most attention and resources (for reaction and prevention).

The *cost-benefit analysis*, as the third part of the risk analysis approach to cybersecurity, brings the issues of acceptable risk and the value of a saved life together. The conventional approach compares the costs of the security measure with its benefit in the lives saved and damages averted. The benefit of a security measure is a multiplicative composite of three considerations: a) the probability of a successful attack absent the security measure; b) the losses sustained in a successful attack; and c) the degree to which the security measure reduces the risk by lowering the probability and/or the consequences of a successful attack.[568] If the benefit of the risk-reduction measure is greater than its cost, then the measure is deemed cost-effective. With certain cybersecurity threats or types of attack, usually those perceived as most dreadful (such as cyberwarfare and cyberterrorism), there is a lack of past experience. As such, the likelihood of such events in the future is very difficult to discern. This is another reason why these types of attacks should not be the *primary* focus of cybersecurity as a concept and cybersecurity governance measures in practice.

The last part of the risk analysis approach is *risk communication*. This means that regulators who seek to expand limited funds in a manner that best enhances security should be risk neutral –

[565] For the US Elisabeth Paté-Cornell found these numbers to be up to $1 million (that is how much the regulators are in general prepared to pay to save a life) and up to $10 million (above which the regulators would rather expend funds on measures that save lives at a lower cost); the maximal cost per saved life is much higher when it comes to dread risks such as terrorism and can be up to $7 or even 14 million; CATO, p. 4.
[566] Mueller and Stewart 2014, p. 6.
[567] If the attack centres on a critical infrastructure the consequences can range from mild annoyance to more serious effects, depending on which part of the infrastructure is affected in what way and for how long.
[568] Mueller and Stewart 2014, p. 7.

in as far as this is possible. This implies that they should deal with the objective likelihood that the hazard will occur and rely on that in their decision-making (rather than on worst-case or overly pessimistic scenarios).[569] Here, again, the great psychological, social, cultural and institutional factors connected to dread risks arise – regulators are incentivised to communicate risk in line with the public's (exaggerated) expectations and react in an exaggerated manner to them as well. More realistic communication to the public (and then action taken in accordance with it) does not necessarily mean that the official will not be re-elected for not acting in line with the public's (initial) expectations.[570]

According to these four steps in a risk analysis approach to cybersecurity policy and action, cybersecurity threats that are likely to occur and to incur non-acceptable damages (as defined at a certain time and place[571]) should be given priority, as that is the most responsible thing to do. Moreover, the occurrence of a new attack, despite measures taken based on such a risk analysis, should not be *a priori* considered as a failure of the approach. As James Fallows pointed out, political incentives here work only one way: “a politician who supports more extravagant counterterrorism measures can never be proven ‘wrong’, because an absence of attacks shows that the ‘measures have *worked*,’ whereas a new attack shows that we ‘must go further still.’”[572] Admittedly, risk and cost-benefit analysis should not be the sole criteria for public decision-making regarding cybersecurity or other matters. Nevertheless, they provide important insights into how security measures may (or may not) perform, the effect of such measures on risk reduction and their cost-effectiveness. Ignoring these insights may lead to raising unnecessary fears, wasting scarce resources and ignoring important other problems.[573]

Countries should thus take a realistic approach to risk assessment, risk management and risk communication. While there is a need for proactive solutions that ensure stability over the longer term, at the same time it is important to avoid over-comprehensive approaches (i.e. securing everything Internet) that lack focus and concrete goals. Attention should be paid to high-impact, low-probability events (such as cyberterrorism), but strategically and from a cost-benefit perspective, the main focus ought to be on higher-probability events that have medium or higher impact, such as cybercrime, cyberespionage and attacks on critical infrastructures.[574]

[569] Mueller and Stewart 2014, p. 9.

[570] Think of Michael Bloomberg, former mayor of New York, who in 2007 stated that people should “get a life” and that they have a better chance of being hit by lightning than of being struck by terrorism – he was re-elected; from Mueller and Stewart 2014, p. 10.

[571] See also: Mary Douglas and Aaron Wildavsky, *Risk and Culture*, (University of California Press: 1983), who make the same point in regard to environmental risks, and Broeders 2014.

[572] From Mueller and Stewart 2014, p. 10.

[573] As Elisabeth Paté-Cornell stated in ‘Risk and uncertainty analysis in government safety decisions’; from Mueller and Stewart, p. 13.

[574] After the research for this report was finalized, the OECD published a recommendation on Digital Security Risk Management. The two key recommendations that run through the document, that there is a need to adopt an approach grounded in risk management that incorporates social and economic objectives (rather than merely searching for technical solutions) and that digital security measures should be designed in such a way that the interests of multiple stakeholders are taken into account, are largely in keeping with the conclusions drawn on the basis of this study. See: OECD, ‘Digital security risk management for Economic and Social prosperity,’ 2015.

6.5 Lessons Learned

Based on our findings in the use cases and the approaches discussed in the literature, the following points can be made as lessons learned from our analysis, and thus also as issues that are important for further consideration since they are rather starting points for further reflection and policy development.

1. Do not expect to resolve issues merely by establishing more laws. States currently tend to attempt to resolve cybersecurity problems by increasing 'criminalisation' – i.e. arranging tightening the reins through criminal law – but this is not necessarily the best or only solution. The countries studied here also illustrate alternative routes to regulating the field.

2. The multi-stakeholder, private-public partnership approach is considered to be a crucial characteristic for governing cyberspace. All countries recognize this and this approach is evident in all the cases, albeit in slightly different forms. While there are considerable advantages to such an approach, the disadvantages highlighted here (such as coordination problems) should not be overlooked.

3. In light of point 2, in such arrangements, who is coordinating between stakeholders (including who takes the lead and who has ultimate responsibility) should be clear and formally delineated.

4. Policy makers can increase oversight efforts, which will indicate where there are potential gaps in both systems and the processes that govern them. Especially in differentiated forms of collaboration and cooperation, oversight is crucial.

5. In multi-stakeholder collaborations, especially where certain actions are based on voluntary efforts, trust is a key success factor. Trust cannot be demanded or regulated, but fostered through good communication, information exchange and making clear agreements regarding division of tasks and actions to be taken.

6. Cybersecurity is not necessarily separate from national security or civil protection, but an exceptional case that requires specific attention for the aforementioned points. Countries should carefully consider whether and how they regulate cybersecurity in relation to national security and civil protection: both an integrated governance regime and separate regimes can be employed, but either way, public policy should address the pitfalls in an integrated approach (e.g., too complex or too vague approaches, insufficient attention for the specifics of cybersecurity) or those in a separated approach (e.g., lack of coordination, policy competition, redundancy).

Available online: http://www.oecd-ilibrary.org/science-and-technology/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en.

6.6 Conclusion

In modern societies, non-governmental actors play an increasing role in influencing policy outcomes, whereby the role of the centralized government (and, as such, its relationship to society) continues to change. Most especially, changing dynamics in public-private relationships and influences at the systemic (international) level put the effectiveness and legitimacy of classical policy strategies and instruments up for discussion. The cases discussed in this report provide yet another example of policy challenges for which the solution is often thought to require polycentric governance structures, rather than hierarchical ones. Indeed, developments in the field are dynamic and rapid, often occurring in absence of a central authority to steer or coordinate the process. On the one hand, in such situations, polycentric constellations can open a space for the experimentation and iterative learning processes that are deemed necessary to governance in process and possibly lead to more effective policy action in areas that span multiple sectoral domains. On the other hand, when the exact nature of the coordination structure is unclear, actors become concerned about the respective roles of the different parties (and who will take the lead) in cases of incidents and repression. This can even lead to opposing – rather than coordinated – actions (and in some cases, non-action) owing to individual interests, reflecting the steep learning curve that actors currently face in their efforts to coordinate collective action.

Some uncertainty is evident in the cases examined here, which reflect a great degree of decentralization to sectors that take a risk analysis or problem-oriented approach to dealing with cybersecurity. Decentralization is not necessarily a positive or negative development in and of itself. It seems logical, given the numerous, intertwined, social and technical factors that influence cybersecurity in various layers of society (e.g. data, infrastructure, personal behaviour, etc), that societies would move to governance arrangements that allow for cooperation between public and private parties, often (but not always) underpinned by some form of regulation. Use of contracts is one way of legitimizing cooperation, but may not always provide the desirable level of legitimacy from a public governance perspective. Moreover, many arrangements currently remain ‘voluntary’ or ‘encouraged’ for some actors and – especially because of the multiple layers that must be taken into account – there is an ever-present risk of fragmentation, which could impede effective policy action (gaps in coverage, inefficiency, policy competition, etc.), if the overarching picture is missing. More discussion is needed on how far society wants to proceed in engaging the private sector in public security, and how this can best be regulated.

Bibliography

Annus, R, 'E-residentsus' (2014) 10 Juridica <http://juridica.ee/get_doc.php?id=2160>.

Asselt, M.B.A. van and O. Renn, 'Risk Governance' (2011) 14 Journal of Risk Research 431.

Autoriteit Consument en markt, 'Elektriciteit' <https://www.acm.nl/nl/onderwerpen/energie/elektricitieit/> accessed 18 September 2015.

Baker, S.A. and Filipiak, N. and Timlin, K. *In the Dark: Crucial Industries Confront Cyber Attacks* (McAfee, Incorporated, 2011).

Baker, S.A. and Waterman, S. and Ivanov. G. *In the crossfire: Critical infrastructure in the age of cyber war* (McAfee, Incorporated, 2009).

Bambauer D.E., 'Conundrum' (2011) 96 Minnesota Law Review <http://www.minnesotalawreview.org/wp-content/uploads/2012/02/Bambauer_MLR.pdf> accessed 28 September 2015.

Bipartisan Policy Center, 'Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat, A Report from the Co-chairs of the Bipartisan Policy Center's Electric Grid Cybersecurity Initiative' <http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Cybersecurity%20Electric%20Grid%20BPC.pdf> accessed 18 September 2015.

Blank, R.H. and V. Burau, *Comparative Health Policy* (3rd edition, Houndmills: Palgrave Macmillan 2010).

Brandão L., Christin N. and Danezis G, 'Toward Mending Two Nation-Scale Brokered Identification Systems' (2015) 2 Proceedings on Privacy Enhancing Technologies 135.

Brandsen, T., Donk, W. van de and K. Putters 'Griffins or Chameleons? Hybridity as a Permanent and Inevitable Characteristic of the Third Sector' (2005) 28 International Journal of Public Administration 749.

British Columbia Government, 'BC Services Card' <http://www2.gov.bc.ca/gov/topic.page?id=87EEAD6D19974459950AA7FF7F60AD54> accessed 18 September 2015.

British Columbia Government, 'Criminal Record Checks' <http://www.pssg.gov.bc.ca/criminal-records-review/eiv/index.htm> accessed 18 June 2015.

Broeders, D, 'Investigating the Place and Role of the Armed Forces in Dutch Cyber Security Governance' (2014) Ministerie van Defensie / Erasmus Universiteit Rotterdam.

BSI (Bundesamt für Sicherheit in der Informationstechnik), 'Innovations for an eID Architecture in Germany' (Bonn: BSI 2010).

Bubandt, N, 'Vernacular Security,' 36.3 Security Dialogue 275-296.

Bundesministerium für Wirtschaft und Technologie, 'ICT Strategy of the German Federal Government: Digital Germany 2015' (Munich: BMWi 2010).

Buzan, B., *The United States and the Great Powers: World Politics in the Twenty-First Century* (Polity Press 2004), p. 172.

Buzan, B., Waever O, and de Wilde J, *Security: A new framework for analysis* (Lynne Riener 1998)

Canadian Office of the Privacy Commissioner, 'About the Office of the Privacy Commissioner' <https://www.priv.gc.ca/au-ans/index_e.asp> accessed 18 September 2015

Canadian Office of the Privacy Commissioner, 'Bill S-4, An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another

Act' <https://www.priv.gc.ca/parl/2014/parl_sub_140604_sen_e.asp> accessed 18 September 2015

Canadian Office of the Privacy Commissioner, 'Guidelines for Identification and Authentication' <https://www.priv.gc.ca/information/guide/auth_061013_e.asp> accessed 18 September 2015

Canadian Office of the Privacy Commissioner, 'Reporting breaches under the Privacy Act' <https://www.priv.gc.ca/resource/pb-avp/pb-pa_e.asp> accessed 18 September 2015

Certification Centre, 'About' <https://sk.ee/en/about/>

Citizen-Centred Service Network, 'Public Sector Service Delivery Council (PSSDC)' <http://www.iccs-isac.org/en/councils/pssdc/> accessed 18 September 2015.

Computer Science Telecommunications Board (CSTB), *Computers at risk: Safe computing in the information age* (National Academy Press, 1991).

Corbridge, S., Willams, G, Srivastava, M. and R. Veron, *Seeing the State* (Cambridge University Press 2005).

Cormack, A., 'Can CSIRT Lawfully Scan for Vulnerabilities?' (2014) 11.3 *SCRIPTed* 309.

Cuijpers C, 'Country report eID in the Netherlands' (Working paper, 2014), paragraph 3.2.

Dean Beeby, 'Canada Revenue Agency privacy breach leaks prominent Canadians' tax details' (CBC News, 25 November 2014) <http://www.cbc.ca/news/politics/canada-revenue-agency-privacy-breach-leaks-prominent-canadians-tax-details-1.2849336> accessed 18 September 2015

Digital Identification and Authentication Council of Canada, 'Building Canada's Digital Identity Future' (May 2015)

Douglas, M. and Wildavsky, A., *Risk and Culture* (Berkely: University of California Press 1983).

Dunn Cavelty, M., 'The Militarisation Of Cyber Security As A Source Of Global Tension' (2012) in Möckli, D. (ed) *Strategic Trends and Analysis: Key Developments in Global Affairs* <http://www.css.ethz.ch/publications/pdfs/Strategic-Trends-2012-Cyber.pdf> accessed 28 September 2015.

Elering, 'Electricity System' <http://elering.ee/the-electricity-system/>.

Energiasalv, <http://energiasalv.ee/energiasusteem>

Energie-Nederland, 'Energie-Nederland' <http://www.energie-nederland.nl/aangesloten-energiebedrijven/> accessed 18 September 2015.

Estonian Competition Authority, 'Energy distribution undertakings in Estonia' (2015) <http://www.konkurentsiamet.ee/file.php?27430>.

Estonian Data Protection Inspectorate, 'Isikukoodi kasutamine' ('Guidelines on the Use of the Personal Identification Code') (2013). <http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikukoodi%20kasutamise%20juhend_0.pdf>

Estonian Defence League, 'Estonian Defence League's Cyber Unit' < <http://www.kaitseliit.ee/en/cyber-unit>.

Estonian Information System Authority, 'Actions and Roles of the Department of Critical Information.

Estonian Information System Authority, 'Critical Information Infrastructure Protection' <https://www.ria.ee/CIIP/>.

Estonian Information System Authority, 'Data Exchange Layer X-Road' <https://www.ria.ee/x-road/>.

Estonian Information System Authority, 'ISKE audit' <https://www.ria.ee/iske-audit/>.

Estonian Information System Authority, 'Public Key Infrastructure PKI' <https://www.ria.ee/en/?id=27307>.

Estonian Information System Authority, 'Report of the Cybersecurity Service of the Estonian Information System Authority' (2014), <https://www.ria.ee/public/Kuberturvalisus/RIA-Kyberturbe-aruanne-2014.pdf>.

Estonian Information System Authority, 'Three-level IT baseline security system ISKE' <https://www.ria.ee/iske-en/>.

Estonian Information System Authority, 'Virtual Situation Room' <https://www.ria.ee/vsr/>.

Estonian Ministry of Economic Affairs and Communications, 'Cyber Security Strategy' (2014) <https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf>.

Estonian Ministry of Economic Affairs and Communications, 'Electricity Market' <https://www.mkm.ee/et/tegevused-eesmargid/energeetika/elektriturg>.

Estonian Ministry of Justice, 'Crime in Estonia. 2014' (2015) <http://www.kriminaalpoliitika.ee/sites/www.kriminaalpoliitika.ee/files/elfinder/dokumendid/kuritegevuse_at_2015_0.pdf>.

Estonian Ministry of Justice, 'Criminal Policy Trends up to 2018' (2010) <http://www.just.ee/sites/www.just.ee/files/elfinder/article_files/kriminaalpoliitika_arengusuunad_aastani_2018.pdf>.

European Commission (2013), *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels 7.2.2013, JOIN(2013) 1 final.

European Commission, Eurobarometer, 'Cyber Security' <http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_fact_ee_en.pdf>.

Everett, C. 'Who is responsible for securing critical infrastructure?' (2010) 10 Computer Fraud & Security 5.

Fafinski, S. 'The security ramifications of the Police and Justice Act 2006' (2007) 2 Network Security 8.

German Federal Ministry of the Interior, 'Cyber Security Strategy For Germany' (Federal Ministry of the Interior 2011).

Government of Canada, 'Action Plan 2010-2015 for Canada's Cyber Security Strategy' <http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf> accessed 18 September 2015.

Government of Canada, 'Action Plan for Critical Infrastructure 2014-2017' <http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf> accessed 18 September 2015.

Government of Canada, 'Budget 2015' <http://www.budget.gc.ca/2015/docs/plan/ch4-3-eng.html> accessed 18 September 2015.

Government of Canada, 'Canada's Cyber Security Strategy. For a stronger and more prosperous Canada' <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/canadaNCSS.pdf> accessed 18 September 2015.

Government of Canada, 'The Canadian ePassport' < http://www.cic.gc.ca/english/department/media/multimedia/video/e-passport/e-passport.asp> accessed 18 September 2015.

Hanneli R, 'Elektrinäidu teatamisest saab kahe aasta pärast ajalugu' (2015) <http://tarbija24.postimees.ee/3056155/elektrinaidu-teatamisest-saab-kahe-aasta-parast-ajalugu>.

Helderman, J.K., Bevan, G. and G. France., 'The Rise of the Regulatory State in Healthcare: A Comparative Analysis of the Netherlands, England and Italy' (2012) 7 Health Economics Policy and Law 103.

Hansen, L. and H. Nissenbaum, 'Digital Disaster, Cyber Security, And The Copenhagen School' (2009) 53 International Studies Quarterly.

Highfield, M 'The Computer Misuse Act 1990: Understanding and Applying the Law' (2000) 5.2 Information Security Technical Report 51.

Hirsnik, E. (2014), 'Arvutikuritegevuse regulatsioon Eestis: karistusõiguse revisjoniga toimunud muudatused ja lahendamata jäänud probleemid' 8 Juridica, <http://www.juridica.ee/juridica_et.php?document=et/articles/2014/8/244874.SUM.php>

Hornung G. and A. Roßnagel., 'An ID card for the Internet – The new German ID card with "electronic proof of identity' (2010) 26 Computer Law & Security Review 151.

Horsch, M., Braun, J. and A. Wiesmaier, 'Mobile eID Application for the German Identity Card' (Technical Report, TU Darmstadt 2013).

House of Commons, *Defence and Cyber-security – Written Evidence* (Defence Committee, DCS 001, 2012).

Hout, E. van, Putters, K. and M. Oude Vrielink, 'Governance of Local Care and Public Service Provision' (Paper for the EGPA conference, Madrid, September 2007).

ID, 'Certificates' <http://www.id.ee/index.php?id=30228>

Industry Canada, Digital policy branch: Protecting and managing digital identities online. <https://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00585.html> accessed 18 June 2015

Industry Canada, Digital policy branch: Protéger et gérer les identités numériques en ligne. <https://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/h_gv00240.html> accessed 18 June 2015

Infrastructure Protection at the Estonian Information System's Authority' <https://www.ria.ee/actions-and-roles/>

Institute for Prospective Technological Studies, Information Society Unit, *Minutes from the eId and Law Workshop – Regulatory and legal Aspects of electronic identity (*European Commission, 2009).

ITU (International Telecommunications Union) (2014), *Measuring the Information Society Report 2014*, Geneva: ITU.

Jang-Jaccard, J. and Nepal S. 'A survey of emerging threats in cybersecurity' (2014) 80.5 Journal of Computer and System Sciences 973.

Jenkins, R., The Emergence of the governance agenda: sovereignty, neo-liberal bias and the politics of international development. In: The Companion to Development Studies (Oxford University Press 2002).

Kahu, O., 'Algab kaugloetavate elektriarvestite paigaldamine' (2012) <http://uudised.err.ee/v/majandus/863293ec-14f6-4c8b-9bc9-7f1a2785242f>

Kjær, Anne Mette, *Governance* (Polity Press 2004).

Klimburg A., 'National Cyber Security Framework Manual' (NATO Cooperative Cyber Defense Center of Excellence 2012).

Knight, A. and Saxby S. 'Identity crisis: Global challenges of identity protection in a networked world' (2014) 30.6 Computer Law & Security Review 617.

Koops, B.J. 'Technology and the Crime Society: Rethinking Legal Protection' (2009) 1 Law, Innovation and Technology 93.

Livingstone, D. and Clemente D. and Yorke C. *Cyber security and the UK's critical national infrastructure* (Chatham House, 2011).

Logius, 'Diensten' < https://www.logius.nl/diensten/> accessed 18 September 2015.

Luiijf, H.A.M. et al., 'Ten National Cyber Security Strategies: A Comparison' in Sandro Bologna, Bernard Hämmerli, Dimitris Gritzalis and Stephen Wolthusen (eds.), *Critical Information*

Infrastructure Security (1st edn, Springer 2011) <http://link.springer.com/book/10.1007/978-3-642-41476-3> accessed 28 September 2015.

Macewan, N. F. 'The Computer Misuse Act 1990: lessons from its past and predictions for its future' (2008) 12 Criminal Law Review 955.

McMaster University, Measuring Identity Theft in Canada: 2008 Consumer Survey

Moore, T. 'The economics of cybersecurity: Principles and policy options' (2010) 3.3 International Journal of Critical Infrastructure Protection 103.

Moosavian, R. ''Keep Calm and Carry On': informing the public under the Civil Contingencies Act 2004' (2014) 18.2 The International Journal of Human Rights 178.

Mueller, J. and Sterward, M.G. (2014) 'Responsible counterterrorism policy' 755 CATO Institute Policy Analysis. Available at: http://object.cato.org/sites/cato.org/files/pubs/pdf/pa755.pdf

Netherlands Nationaal Cyber Security Centrum, 'Framework ICT protection assessments for the DigiD' <https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html> accessed on 13 May 2015.

Netherlands Overheid, 'Internetconsultatie: Wet gegevensverwerking en meldplicht cybersecurity' <http://www.Internetconsultatie.nl/cybersecurity> accessed 18 September 2015

Nicholson, A. et al. 'SCADA security in the light of Cyber-Warfare' (2012) 31.4 Computers & Security 418.

Nissenbaum, H. 'Where Computer Security Meets National Security' (2005) 7.2 Ethics and Information Technology 61.

Noack, T. and H. Kubicek. (2010), *The introduction of online authentication as part of the new electronic national identity card in Germany,* Identity in the Information Society, 3(1), 87-110.

Norea, 'NOREA' <www.norea.nl> accessed on 13 May 2015.

OECD, 'Digital security risk management for Economic and Social prosperity' (OECD 2015). http://www.oecd-ilibrary.org/science-and-technology/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en.

OECD, 'National Strategies and Policies for Digital Identity Management in OECD Countries' (OECD Digital Economy Papers, No. 177, OECD Publishing 2011).

Osula, A., 'National Cyber Security Strategy Organisation: Estonia', (CCDCOE 2012) <https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf>

Osula, 'A. National cyber security organisation' (CCDCOE 2015).

Parlement en Politiek, 'Agentschappen (baten-lastendiensten)' <http://www.parlement.com/id/vh8lnhrqszxe/agentschappen_baten_lastendiensten> (in Dutch) accessed on 13 May 2015.

Poller, A., Waldmann, U., Vowé, S. and S. Türpe., 'Electronic Identity Cards for User Authentication – Promise and Practice' (2012) 10 IEEE Security and Privacy 46.

Posadzki, A., 'Cyber Security In Canada's Private Sector A 'Significant' Problem: Government Records' (The Canadian Press, 13 September 2013). <http://www.huffingtonpost.ca/2013/07/14/cyber-security-canada_n_3594310.html> accessed 18 September 2015

Privacy and Consumer Advisory Group (PCAG), 'Identity Assurance Principles' (V3.1. 2014).

RFC 2350 Description for CERT-EE <https://www.ria.ee/public/CERT/CERT-EE_rfc2350.pdf>

Riigikogu, 'Eesti infopoliitika põhialused' (1998) <https://www.riigiteataja.ee/akt/75308>

Rhodes, R.A.W., *Understanding governance: policy networks, governance, reflexivity and accountability* (Open University Press 1997).

Rijksoverheid, ‘Basisregistratie personen (BRP)’ <http://www.rijksoverheid.nl/onderwerpen/persoonsgegevens/basisregistratie-personen-brp> accessed on 13 May 2015.

Rijksoverheid, ‘Veilig omgaan met uw DigiD’ <https://www.digid.nl/veiligheid/> accessed 18 September 2015.

Robinson, N. et al., ‘Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report’ (RAND Europe 2011).

Rosner, G. L., ‘Identity management policy and unlinkability: A comparative case study of the US and Germany’ (University of Nottingham 2014).

Royal Canadian Mounted Police, ‘Cybercrime: an overview of incidents and issues in Canada’ <http://www.rcmp-grc.gc.ca/pubs/cc-report-rapport-cc-eng.htm> accessed 18 September 2015.

Royal Canadian Mounted Police, ‘Cybercrime: an overview of incidents and issues in Canada’ <http://www.rcmp-grc.gc.ca/pubs/cc-report-rapport-cc-eng.htm> accessed 18 September 2015.

Royal Canadian Mounted Police, ‘Identity Theft and Identity Fraud Victim Assistance Guide ’<http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-eng.htm> accessed 18 September 2015.

Sabel, C.F., ‘Experimentalist Governance’, in: Levi-Fleur, D. (ed.) *The Oxford Handbook of Governance* (Oxford University Press 2012).

Saxby, S. ‘The 2013 CLSR-LSPI seminar on electronic identity: The global challenge–Presented at the 8th International Conference on Legal, Security and Privacy issues in IT Law (LSPI) November 11–15, 2013, Tilleke & Gibbins International Ltd., Bangkok, Thailand’ (2014) 30.2 Computer Law & Security Review 112.

Saxby, S. ‘The 2014 CLSR-LSPI Lisbon seminar on ‘the digital citizen’–Presented at the 9th International Conference on Legal, Security and Privacy Issues in IT Law (LSPI) 15–17 October 2014, Vieira De Almeida & Associados, Lisbon, Portugal’ (2015) 31.2 Computer Law & Security Review 163.

Segers, J. and J. Hutjes., *De gevalstudie. Methoden voor de Maatschappijwetenschappen* (Assen: van Gorcum 1999) Chapter 11, pp 339-366.

Smedinghoff, T. J. ‘Solving the legal challenges of trustworthy online identity’ (2012) 28.5 Computer Law & Security Review 532.

Spanish Cyber Security Institute, 'National Cyber Security, A Commitment For Everybody' (Spanish Cyber Security Institute 2012).

Statistics about Internet Voting in Estonia <http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics>.

Streeck, W. and W.C. Schmitter., ‘Community, Market, State and Associations? The Prospective Contribution of Interest Governance to Social Order’ (1985) 1 European Sociological Review 119.

Sullivan, C. ‘Digital identity–The legal person?’ (2009) 25.3 Computer law & security review 227.

Tenbensel, T., ‘Multiple Modes of Governance’ (2005) 7 Public Management Review 267.

Tennet, ‘Over TenneT’ <http://www.tennet.eu/nl/nl/over-tennet.html> accessed 18 September 2015.

Tennet, ‘Programmaverantwoordelijkheid’ <http://www.tennet.eu/nl/nl/klanten/diensten/syteemdiensten/programmaverantwoordelijkheid.htm> accessed 18 September 2015.

Tjong Tjin Tai, T.F.E. et al., *Duties of Care and Diligence Against Cybercrime* (Wolf Legal Publishers 2015).

Treasury Board of Canada Secretariat , 'Directive on Identity Management' <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577> accessed 18 September 2015.

Treasury Board of Canada Secretariat, "Standard on Identity and Credential Assurance" <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776> accessed 18 September 2015.

Tuohy, C.H., 'Agency, Contract, and Governance: Shifting Shapes of Accountability in the Health Care Arena' (2003) 28 Journal of Health Politics, Policy and Law 195.

UP Kritis Public-Private Partnership for Critical Infrastructure Protection, Basis and Goals (2014). http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/UP%20KRITIS.pdf;jsessionid=D0C57276FEE2B176F8AAF008569D9A9B.1_cid320?__blob=publicationFile.

UK Cabinet Office *Cyber Security Strategy of the United Kingdom – safety, security and resilience in cyber space* (2009).

UK Cabinet Office *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review* (2010).

UK Cabinet Office *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards* (2010).

UK Cabinet Office *The UK cyber security strategy–protecting and promoting the UK in a digital world* (2011).

UK Cabinet Office, *National Risk Register* (2008, 2010, 2012, 2015).

UK CESG and Cabinet Office *Good Practice Guide No. 43 – Requirements For A Secure Delivery Of Online Public Service* (Issue No 1.1, 2012).

UK CESG and Cabinet Office *Good Practice Guide No. 44 – Authentication and Credentials for use with HMG Online Services* (Issue No 2.0, 2014).

UK CESG and Cabinet Office *Good Practice Guide No. 45 – Identity Proofing and Verification of an Individual* (Issue No 2.3, 2014).

UK CESG and Cabinet Office *Good Practice Guide No. 46 – Organisation Identity* (Issue No 1.0, 2013).

UK CESG and Cabinet Office *Good Practice Guide No. 53 – Authentication and Credentials for use with HMG Online Services* (Issue No 1.0, 2013).

UK Parliamentary Office of Science & Technology (POST) *Managing Online Identity* (Postnote Number 434 2013).

Van den Berg, J. and others, 'On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education' (NATO STO/IST-122 symposium, Tallinn, 13-14 October 2014) available at https://www.csacademy.nl/images/MP-IST-122-12-paper-published.pdf

Verkade T, 'Massafraude met belastingtoeslagen via DigiD' (*NRC,* 19 September 2011) <http://www.nrc.nl/nieuws/2011/09/19/massafraude-met-belastingtoeslagen-via-digid/> accessed 13 May 2015.

Von Solms, R. and Van Niekerk J. 'From information security to cyber security' (2013) 38 Computers & security 97.

Wall, D., *Cybercrime* (1st edn, Polity 2007).

Walton, R. 'The Computer Misuse Act' (2006) 11.1 Information Security Technical Report 39.

Williams, M.C., *Culture and Security: Symbolic Power and the Politics of International Security* (Routledge 2007).

Wood, A., 'Resilience of the Critical National Infrastructure' (Ogres 2008) <http://www.orgres.co.uk/documents/doc_download/34-wp-01-resilience-of-the-critical-national-infrastructure> accessed Jun. 2015.

Worthy J. and Fanning M., ‘Denial-of-Service: Plugging the legal loopholes?’ (2007) 23.2 Computer Law & Security Review 194.

Appendix 1. List of Abbreviations Used

ACM	Authority for Consumers and Markets (NL)
BKA	Federal Criminal Police Office (DE)
BSI	Federal Office for Information and Security (DE)
C&C	Command and Control
CC III	Computercriminaliteit III (NL)
CCIRC	Canadian Cyber Incident Response Centre
CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CiSP	Cyber-security Information Sharing Partnership (UK)
CMA	Computer Misuse Act (UK)
CSIRT	Computer Security Incident Response Team
CSTB	Computer Science and Telecommunications Board
CVCA	Country Verifying Certificate Authority (DE)
DDoS	Distributed Denial of Service
DoS	Denial of Service
EC3	European Cyber Crime Centre
ENISA	European Union Agency for Network and Information Security
EU	European Union
FBI	Federal Bureau of Investigation (US)
FIRST	Forum of Incident Response and Security Teams
GCPC	German Criminal Procedure Code
IAA	Identification, authentication and authorization
ICS	Industrial Control System
ICT	Information and Communication Technology
ISA	Information System Authority (EE)
ISAC	Information Sharing and Analysis Center
ISP	Internet Service Provider
ITU	International Telecommunication Union
J-CAT	Joint European Cybercrime Action Task Force
MEAC	Ministry of Economic Affairs and Communications (EE)
NATO	North Atlantic Treaty Organization
NCA	National Crime Agency (NCA)
NCCU	National Cyber Crime Unit (UK)
NCS	National Cybersecurity Strategy
NCSC	National Cyber Security Centre (NL)
NCSS 2	National Cyber Security Strategy 2 (NL)
NCTV	National Coordinator for Security and Counterterrorism (NL)
NERC	North American Electric Reliability Corporation (C)
NFI	National Forensics Institute (NL)
NGO	Non-governmental Organization
NHTCU	National High Tech Crime Unit (NL)
NIS	Network and Information Security
NRR	National Risk Register for Civil Emergencies (UK)
P2P	Pollution Prevention Progress
PPP	Public-Private Partnership
SCADA	Supervisory Control And Data Acquisition
TERENA	Trans-European Research and Education Networking Association
TI	Trusted Introducer for European CERTs
TOR	The Onion Router
VSR	Virtual Situation Room (EE)
WID	Warning Information Service (DE)

Appendix 2. List of Interviewed Experts

Canada

Martin Rudner, Ph.D., Distinguished Research Professor, Emeritus, Carleton University Ottawa

Estonia

Urmo Sutermäe - Head of the Division of Protection of Critical Infrastructures, Risk Management Division of the Estonian Information Systems Authority

Marek Vasar – Head of the Division of Security and Coordinator of Information Security of State Agencies through IT Baseline Security System ISK, Risk Management Division of the Estonian Information Systems Authority

Janek Rozov - Head of the Department of Information Society Services Development, Ministry of Economic Affairs and Communications

Germany

Gerrit Hornung – Chair of Public Law, IT Law and Legal Informatics, Institute of IT-Security and Security Law (Uni Passau)

United Kingdom

Ian Brown – Professor of Information Security and Privacy, Oxford Internet Institute

George Danezis – Reader in Security and Privacy Engineering, Information Security Group, Computer Science Department, University College London

Eerke Boiten – Senior Lecturer, School of Computing, University of Kent

Appendix 3. Advisory Committee Members

prof.dr.ir. J. van den Berg (chair)	Delft University of Technology
prof.dr. D.W.J. Broeders (co-chair)	Erasmus University Rotterdam / WRR (Scientific Council for Government Policy)
dr.ir. R. Choenni	WODC
drs. J.P. Hondebrink / R. van der Luit	Ministry of Economic Affairs
drs. M.H.G. van Leeuwen	Ministry of Security and Justice
dr. J.B.J. van der Leij, LL.M.	WODC
M. Steltman	Dutch Hosting Provider Association