Thesis

MSc Crisis and Security Management

Supervisor: dr. E. De Busser

University of Leiden

Resilience as Security in European Cyberspace

How the Netherlands and France are moving towards open and adaptable cybersecurity systems

by

Anton Wuis

s1379747

a.wuis@umail.leidenuniv.nl

Submitted: July 23rd, 2020

Word count: 16.002 (including citations)

Contents

Introduction

Jean-Claude Juncker, in his 2017 State of the Union Address stated that "Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks," hereby identifying cybersecurity as one of the Union's policy priorities for the coming year (Juncker, 2017).[1] However, a large number of challenges still remain, including a fragmented institutional landscape and the lack of binding legal norms (Carrapico & Barrinha, 2018). Despite these challenges and the complexities surrounding European Union competence in the field of cybersecurity, the EU has presented itself as a logical forum to address cybersecurity threats due to their transboundary nature (European Commission, 2013). There is no single legal basis for EU competence in the field of cybersecurity. Instead, cybersecurity policy is connected to existing competences such as the internal market or put forward in soft law instruments (Wessel, 2015, p. 405). The European Union Cybersecurity Strategy (EUCSS) therefore recognises that the task of addressing the challenges in cyberspace predominantly lies with the member states (European Commission, 2013, p. 4).

A search through the 27 national cybersecurity strategies of European Union member states published in English and the EU Cybersecurity Strategy reveals the mention of the term 'resilience' 124 times in 23 different strategies.[2] Whereas resilience in the cybersecurity strategy of Finland refers to, among others, the psychological resilience of its population to crisis (Ministry of Defence, 2013), the Portuguese strategy speaks of resilience of critical infrastructure (Governo de Portugal, 2015). In the Romanian strategy, resilience is used to describe its overall goal of creating a resilient virtual environment, but also taken as an objective for its critical infrastructure (Guvernul României, 2013). In relation to the use of the term in the EU context, the European Data Protection Supervisor has noted that the lack of clarity of the term resilience is an important weakness of the European Cybersecurity Strategy (Hustinx, 2013, p. 2). This widespread use of the term signifies two developments in cybersecurity policy, namely that 'resilience' in cyberspace is an important aspiration to many member states, but also that there is an inherent conceptual opaqueness as to what the concept signifies.

[1] The prefix "cyber-" is attached to suffices in different iterations. Renditions such as cyber security, as well as cybersecurity and cyber-security are all used in the source material. In this thesis, "cybersecurity", "cyberspace", etc. are used, following the Merriam Webster and Oxford dictionaries. Divergent spellings found in quotations and document titles are written in their original style.

[2] The national cybersecurity strategies of all EU member states can be found on the ENISA website, https://www.enisa.europa.eu/topics/national-cyber-security-strategies. This search was carried out on the documents as retrieved on April 6th, 2019.

George Christou (2016), in discussing resilience in cyberspace within the European Union has put forward a framework for assessing what form of resilience characterises a 'cybersecurity ecosystem' and the processes underlying this development (p. 5). In developing his framework, he draws from parallel research on resilience and security governance to arrive at a conceptualisation of what he calls 'effective' resilience as security in cyberspace (Christou, 2016, p. 29). 'Cyber-resilience' is still a relatively underdeveloped concept in the academic literature, as it can be used to discuss resilience of computer networks (Tran et al., 2016), malware risk management techniques (de Crespigny, 2012), or resilience of 'smart' airport cybersecurity systems (Lykou et al., 2018). Although the framework provided by Christou (2016) needs more empirical underpinning, it provides a coherent structure for discussing the different conceptualisations of the term and how policy can contribute towards achieving resilience in cyberspace. For an analysis of French and Dutch cybersecurity approaches, the research draws on and expands the extended typology of Handmers and Dovers (1996) that Christou (2016) puts forward.

Through a comparative case study of the development of cybersecurity strategies and policies of two member states with a more advanced cybersecurity approach, this research aims to shed light on what it means to achieve resilience in cyberspace and the pathways towards doing so. For these purposes, the research takes a causal-process tracing approach, mapping out the evolution of policies in the field of cybercrime and military cyberdefence. The goal is not to put forward the French or Dutch conceptualisations of resilience, but rather to place the term in a wider academic debate on resilience in cyberspace and to explicate the extent to which these two states are in a position to develop resilience in their cybersecurity efforts. Although this research is not directly focused on EU cybersecurity policies, it does aim to place the Dutch and French efforts in their wider European context.

The research question underpinning this thesis is formulated as follows. *To what extent have France and the Netherlands achieved resilience in their cybersecurity approaches, as defined by Christou (2016)?* This question can further be divided into two sub-questions. *As what type of resilience can the French and Dutch approaches be characterised? What are the pathways that have led to their respective approaches to cybersecurity?* With France and the Netherlands as positive cases, given the relatively advanced state of their cybersecurity policies and their diverging institutional cultures, the following hypothesis can be formulated. *H: France and the Netherlands have achieved openness and adaptability in their approach to cybersecurity, but have developed different pathways toward this outcome.* By testing this hypothesis, the research can make a contribution towards the clarification of the term resilience

in cybersecurity literature and hopefully provide an empirical testing of the conditions in the resilience model of Christou (2016), as well as expand on them. Moreover, through an analysis of best practices and shortcomings in the cybersecurity approaches of France and the Netherlands, the research aims to shed light on an evolving body of literature concerned with discussing resilience in national cybersecurity policies (cf. Carr, 2016; Demchak, 2012; Dunn-Cavelty & Suter, 2009; ENISA, 2012; Sliwinski, 2014).

Through demonstrating the applicability of this model by analysing the cybersecurity landscapes and narratives of the Netherlands and France, this research demonstrates that both cases employ a mixed-model approach that is converging towards a type-3 model in recent years. France and the Netherlands have had different starting points and logics underpinning their approach, but their recent convergence raises questions concerning the state of the wider European cybersecurity ecosystem. Further research on the influence member states and the EU have on each other in formulating principles for national cybersecurity strategy has the potential to illustrate how norm-setting has contributed to possible convergence on these principles.

Security as resilience in EU cyberspace

In discussing the importance of and the technical challenges to achieving resilience of networks and the global internet system, Sterbenz et. al (2010) define resilience as "the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation" (p. 1246). ENISA, the EU cybersecurity agency, adopted this definition of resilience and recognised its dual meaning, namely that of resilience as adaptation and resilience as survival (ENISA, 2011, p. 16). This section aims to provide an overview of the different conceptualisations of this broadly used concept. Special attention is paid to how cybersecurity is perceived within the EU context and what the conditions are under which resilience in cyberspace can be achieved.

Conceptualising cybersecurity within an EU context

Before addressing the logics of resilience, it is necessary to arrive at a conceptualisation of cybersecurity given the unclear nature of the term and its different manifestations. In specific, this section focuses on how cybersecurity is defined in the European context. Despite a comprehensive attempt by the International Telecommunication Union (ITU) to provide a common, global definition of cybersecurity (ITU, 2008, p. 2), states have continued to interpret the

concept differently. In part, this divergence can be explained due to countries establishing cybersecurity policies in line with their national interests instead of reinforcing international governance of the internet (E Silva, 2013).

In parallel to fundamental questions in security research (Baldwin, 1997), Carr (2015) seeks to conceptualise cybersecurity in the UK and US strategies by answering the questions of 'cybersecurity for whom? from what? and by what means?' (p. 50). In the EU cybersecurity strategy, the actors called to action by the Commission include ENISA, the member states, the EU itself and industry (European Commission, 2013, p. 8). Nonetheless, the strategy recognises as referent objects in need of security individual citizens as well (p. 4). Cybersecurity from what? refers to the actors from which cyberthreats emanate. Here, the strategy recognises a wide variety of origins, including criminals, state-sponsored attacks and unintentional mistakes (European Commission, 2013, p. 3). Finally, the means by which the EU seeks to achieve cybersecurity can best be described as facilitating and coordinating member state initiatives and furthering EU values while fostering sense of shared responsibility (p. 3-4).

Consolidation efforts by the EU have mainly focused on three issues within cybersecurity. These are countering cybercrime, the protection of critical infrastructure and building cyberdefence capacities within the context of the CSDP (Carrapico & Barrinha, 2017, p. 1260). Aside from these, the EU is active in the field of network and information security and international cybersecurity cooperation (Christou, 2016). In researching the resilience of cybersecurity policy of France and the Netherlands, their interpretation of these issues in their national strategies serves as a red line throughout the analysis. Despite the consolidation efforts by the European Union, developing its cybersecurity policy has been an arduous feat, given the intergovernmental nature of some of the policy areas and a lack of collective vision from its member states (Bendiek et al., 2017; Sliwinski, 2014, p. 480).

Resilience: meanings and typology

Although resilience is defined differently in different academic fields, ranging from psychology (cf. Luthar, 2003) to ecology (cf. Folke, 2006), it is possible to discuss the general meaning of the concept. In essence, it refers to the ability of a someone or a something to remain stable or to 'jump back' in the event of a surprise (Longstaff, 2005, p. 6). The dichotomy between resilience as adaptation and as survival has seen a parallel discussion in the literature on resilience of ecosystems. In discussing these two aspects of resilience, Holling (1996) argues that *engineering* resilience relates to the capacity of a system to return to a stable state after a shock (p. 33). This can be related to the concept of resilience as survival. Systems

designed for this purpose try to anticipate disruptions, leaving them vulnerable to circumstances that are not foreseen (De Bruijne et al., 2010, p. 18).

In contrast, *ecological* resilience assumes that a stable state is irrelevant, given that it is concerned with how much disturbance a system can absorb before it changes its structure or logic, effectively creating a different equilibrium (Holling, 1996, p. 33). This relates to the interpretation of resilience as adaptation. Such an interpretation assumes that, due to the inherent complexity of a system, creating resilience relies on the ability to learn and adapt to consequences rather than to return to an assumed original state as soon as possible. By some authors, the 'success' of the concept of resilience in governance theories is ascribed to its closeness to these neoliberal ideas of complex, adaptive systems (Joseph, 2013; Walker & Cooper, 2011). In line with these complex systems theories are interpretations of resilience in the security studies literature.

The language of resilience, both of technical and social systems, is increasingly permeating national security policies (Dunn Cavelty & Prior, 2013). However, it is important to note that here again, different meanings are ascribed to the concept depending on the context in which it is used. It could relate to engaging members of the public in the provision of security (e.g. through warnings concerning unattended luggage) or to restoring critical infrastructure after a shock. Nonetheless, a common denominator in these approaches can be identified. Most security as resilience processes involve drafting policies and strategies on national levels, while decentralising responsibility to local networks of authority and non-governmental actors (Coaffee & Fussey, 2015, p. 87). It is precisely such networked partnerships that, according to Christou (2016), can contribute to security as resilience in cyberspace (p. 29).

In an attempt to characterise and analyse the cybersecurity governance of the EU, Christou (2016) lays out a framework for discussing conditions for effective security as resilience within EU cyberspace. Based on the topology of resilience by Handmer and Dovers (1996), Christou articulates three distinct types of approaches towards achieving resilience and their respective governance preferences (2016, pp. 25-28). Type 1, Resistance and Maintenance, involves hierarchical governance and state control over resource allocation and information. Specifically, such approaches focus efforts on maintaining the status quo by resisting change. This lack of flexibility can create an outward projection of stability, but the inherent rigidity could also cause long-term damage or even contribute to system collapse.

As for type 2 approaches, Change at the Margins, these are more in line with risk management strategies. Change in such models comes as a result of problem-solving, i.e. addressing issues or symptoms that might arise without thorough consideration of their underlying

causes. This dominant approach presents an inherent danger, namely that incremental change in the short term gives the impression that 'something is being done', while delaying transformational change that could be necessary to address root causes in the long term (Handmer & Dovers, 1996, p. 501). Characterised by a focus on efficiency, type 2 approaches can be perceived as pragmatic as well as politically and economically palatable (Christou, 2016, p. 27).

In contrast to types 1 and 2, type 3, Openness and Adaptability, is characterised by flexibility and a preparedness to move into a different direction by adopting new institutional structures and assumptions. In terms of governance, Christou (2016, p. 27) argues that these approaches involve a broad inclusion of stakeholders and non-hierarchical governance. It assumes that networks of actors coordinate their efforts to build flexible and adaptive institutions and policies in order to accommodate change. Increased costs and inefficiencies arising from a diversity of actors are identified as the main risks of type 3 resilience (Handmer & Dovers, 1996, p. 503). Although Christou does not explicitly justify why, he interprets type 3 resilience as meaning effective security as resilience (2016, p. 30). Nonetheless, arguments can be put forward as to why a focus on flexibility and adaptability might be a more beneficial approach to increasing resilience in areas of cybersecurity as opposed to command-and-control or problem-solving approaches.

Taking into account the complexity of risks and networks within the context of cybersecurity, owed in part to the multiplicity of stakeholders involved, two arguments in favour of a type 3 resilience model can be identified. Firstly, given the unclear nature of threats in cyberspace and the difficulties in calculating the likelihood of a threat occurring and even its impact, linear risk assessment methodologies (type 2) prove to be fundamentally flawed (Dunn Cavelty, 2013, p. 5). Secondly, this complexity and the driving role of the private sector in cybersecurity technology has led to a situation where the government simply does not have the required specialised knowledge to, for example, assess the quality of protective measures for critical infrastructure providers (Dunn-Cavelty & Suter, 2009, pp. 182–183). Therefore, governments do not have the necessary information or technical resources to implement a type 1 model of resilience as this model relies on state control over such information and resources.

Conditions for achieving resilience as security in cyberspace (Christou, 2016, p. 29)

1) Ability (including resource and mandate) and preparedness to adopt new basic operating assumptions and institutional structures;
2) Assumption of efficiency abandoned in favour of complexity in governance logics in order to avoid single points of threat and failure;
3) Coalitions of actors working together in 'partnerships' based on trust to share information, construct new flexible and adaptive institutions and operating procedures, set the agenda and construct/implement policies;
4) Convergence amongst stakeholders on a 'common' understanding, logic(s), 'norms', laws and standards of security as resilience;
5) Evolution of a culture of cybersecurity at all levels and layers (technical, legal, policy) among all stakeholders (awareness, education, learning and so on);
6) An integrated approach (coherence and consistency across layers, levels, actors).

Figure 1

Conditions for type 3 resilience as security in cyberspace

Christou (2016) gives six conditions for achieving what he describes as 'effective' (p. 29) or even 'highly effective' (p. 33) security as resilience in cyberspace. These are listed in figure 1. Although these conditions provide in part the methodological context of this research, their theoretical implications need further discussion. Two main criticisms stand out, the first related to the adjective 'effective' and the second to the lack of empirical grounding of these conditions. Nonetheless, if these conditions are not regarded as benchmarks but rather as indicators of a prevalent resilience type, their value for this research becomes apparent.

How to judge or measure the effectiveness of national cybersecurity policies can take several forms, depending on the background of the researcher. Whereas some authors emphasise the importance of addressing cyberpower in achieving effective cybersecurity policy (Betz & Stevens, 2011; Dunn Cavelty, 2018), others stress the need for coherent or integrated approaches (Carrapico & Barrinha, 2017; Hadji-Janev, 2014). In a similar vein, the effectiveness of different forms of public-private partnerships in the field of cybersecurity provides ground for debate, although their necessity is often undisputed (Bossong & Wagner, 2017; Carr, 2016; Dunn-Cavelty & Suter, 2009). As such, this research does not purport to provide an assessment of the effectiveness of the cybersecurity strategies and policies of the Netherlands and France,

but rather focuses on the extent to which these conditions are present and in how far their respective governments deem them necessary for building a resilient cyberspace.

Secondly, the conditions laid out by Christou (2016) are theoretically informed rather than empirically driven. Indeed, as the author recognises, this means that although general trends and patterns can be identified, an accurate measurement of these conditions proves to be difficult (Christou, 2016, p. 186). In the field of cybersecurity, however, information on the nature of threats and their likelihood of occurrence as well as on the required measures to counter these is as of yet inaccurate (Dunn Cavelty, 2013). For this reason, a further elaboration on the existence of these conditions and trends in the cybersecurity policies of France and the Netherlands could contribute to an assessment of the explanatory value of security as resilience. This question, as well as the incompleteness of available data, is addressed in the following section of the research where these conditions are further problematised.

Research design

In research relating to European Union member states, there exists an inherent trade-off between large-*n* studies that focus on few variables or processes and small-*n* research that provides a more in-depth understanding of causal mechanisms. Given that this research is concerned with characterising the logics of resilience underlying member states' cybersecurity policies, requiring a broad analysis of policies enacted and their motivations, the research is designed as a comparative case study. After discussing the comparative within-case analysis method, this section justifies the selection of France and the Netherlands as positive cases. Finally, attention is paid to data collection, as well as the potential generalisability of the research outcomes.

With the research goal of characterising the form that member states' cybersecurity regime has taken and with their respective pathways for doing so in mind, it is evident that the phenomenon, national cybersecurity policy, is embedded within its wider national context. This national context consists of bureaucratic traditions, individual cyberthreats, the availability of resources, political discourses, EU relations and others. For research where context is highly relevant to discussing a phenomenon, case studies constitute a valuable method to do so (Yin, 2003, p. 13). An explicit choice is made for a comparative research between two cases, as this fortifies the theoretical implications of the findings. If a causal mechanism is found in two relatively similar cases, it is more likely to be generalisable. Moreover, controlling for another case can contribute to explaining possible unexpected outcomes.

In asking how the outcome (resilience type 1, 2, 3 or a mix of these) came to be, causal-process tracing provides a means to reveal the mechanisms that led to this outcome (Blatter & Haverland, 2012, p. 14). In other words, it becomes feasible to address not only *what* France and the Netherlands implemented in terms of cybersecurity policy, but also *how* they did so and what motivated them. In practice, this translates to identifying factors that indicate the presence of the conditions for type 3 resilience as security in cyberspace, as iterated above. The remainder of this section of research design is concerned with operationalising these conditions and illustrating the types of sources in which these can be found.

As the research by Christou (2016) does not provide set indicators for identifying these conditions, a turn to the literature on resilience as well as on cybersecurity is able to provide background as to how these conditions can be operationalised. Moreover, ENISA (2012) has released a set of guidelines for drafting national cyber security strategies that mirror some of the conditions outlined by Christou (2016) on the basis of which indicators for this research can be formulated.

Operationalisation of conditions

Variables such as the existence of a 'common' understanding of security as resilience or the evolution of a cybersecurity culture on all levels are especially difficult to quantify and measure on the basis of numerical data and indicators. Therefore, a set of indicators on the basis of questions has been developed to serve as identifiers of the conditions in figure 1. It is important to note that this research is not concerned with codifying 'yes' and 'no' answers to these questions, as that would prejudice the inherent complexity of analysing the cybersecurity strategies and regimes of France and the Netherlands. Nonetheless, these indicators serve as useful guidelines for conducting this research and as a justification of how the analysis is conducted. An overview of the conditions, their indicators and the academic sources justifying these is given in the operationalisation table in figure 2.

The first condition is concerned with the extent to which a cybersecurity approach creates fundamentally new institutions that function under new operating assumptions. Demchak (2012, p. 132) discusses how then-new cybersecurity organisations were slowly recognising that the provision of national cybersecurity required different operating assumptions than traditional national security approaches did, such as the recognition that cybersecurity is pervasive in every domain of traditional warfare. For the analysis, this means that a discussion is required about the extent to which national cybersecurity institutions are willing to forego traditional security focuses and the extent to which they can adapt themselves to changing circumstances.

A main identifier of type 3 resilience, Openness and Adaptability, is the extent to which a system creates redundancy and flexible allocation of resources, moving away from previous assumptions that organisations should operate as resource-efficient as possible (Dunn Cavelty, 2013, p. 5; Handmer & Dovers, 1996, pp. 492–493). Identifying these criteria provides a lens to discuss whether or not the assumption of efficiency is abandoned in favour of complexity in governance logics (condition 2).

As elaborated upon in the theoretical framework, public-private partnerships are recognised as an essential part of an effective national cybersecurity approach. In light of the type 3 resilience categorisation, discussing the nature of active and proposed partnerships in terms of their hierarchical relations, responsibilities and mandates provides the background to analysing the presence of the third condition. For convergence among stakeholders, a more subjective condition, it is possible to witness the extent to which governments aim to facilitate shared definitions of cybersecurity-related concepts (E Silva, 2013) and if cybersecurity policies correspond with norms set out in cybersecurity strategies.

The fifth condition relates to the creation of a culture of cybersecurity. This can be interpreted as the extent to which a government aims to raise awareness concerning cybersecurity issues among layers of its society, including individuals, the private sector and the public sector (ENISA, 2012, p. 21). Moreover, an emphasis on learning and learning to learn is a key identifier of a type 3 resilient system that focuses on flexibility and adaptability (Wildavsky, 1988, in Handmer & Dovers, 1996, p. 492). Finally, an integrated approach constitutes the sixth condition. This entails coherence in policy and norms in all aspects of a state's cybersecurity approach. Carrapico and Barrinha (2017), in discussing the coherence of EU cybersecurity policy, set out criteria for assessing national cybersecurity policies (p. 1258). These include coordination of policies and instruments between and across national and private levels.

Conditions for type 3 resilience as security in cyberspace: operationalisation table		
Conditions	Indicators	Justification
1) Ability (including resource and mandate) and preparedness to adopt new basic operating assumptions and institutional structures;	a) Does the regime create a fundamentally new institutional structure? b) Which operating assumptions drive these structures?	(Demchak, 2012, p. 132)

2) Assumption of efficiency abandoned in favour of complexity in governance logics in order to avoid single points of threat and failure;	a) Does the funding leave space for redundancy? b) Is there room for flexible allocation of resources?	(Handmer & Dovers, 1996, pp. 492–493) (Dunn Cavelty, 2013, p. 5)
3) Coalitions of actors working together in 'partnerships' based on trust to share information, construct new flexible and adaptive institutions and operating procedures, set the agenda and construct/implement policies;	a) Are the policies realised through localised networks? b) Is governance dispersed across actors and sectors? c) Do partners share information on the basis of trust (voluntarily) rather than on a coercive basis?	(Coaffee & Fussey, 2015, p. 94) (Ibid.) (Carr, 2016, p. 58)
4) Convergence amongst stakeholders on a 'common' understanding, logic(s), 'norms', laws and standards of security as resilience;	a) Does the government aim to create a common understanding of definitions relating to cybersecurity? b) Do the cybersecurity policies correspond with the stated norms?	(E Silva, 2013; ENISA, 2012, p. 1)
5) Evolution of a culture of cybersecurity at all levels and layers (technical, legal, policy) among all stakeholders (awareness, education, learning and so on);	a) Do the cybersecurity policies aim to increase awareness of cybersecurity issues? b) Is there an emphasis on learning in decision-making structures?	(ENISA, 2012, p. 21) (Wildavsky, 1988, in Handmer & Dovers, 1996, p. 492)
6) An integrated approach (coherence and consistency across layers, levels, actors).	a) Are the cybersecurity-related institutions coordinating policies and instruments? b) Do private companies coordinate in the area of cybersecurity?	(Carrapico & Barrinha, 2017, p. 1258)

Figure 2

Case selection: France and the Netherlands as positive cases

Two factors drive the selection of France and the Netherlands as case studies for this research. First, in order to conduct a thorough causal-process tracing analysis of a country's cybersecurity policy to identify the type of resilience as security underlying its approach and to come to a deeper understanding, a large variety of empirical sources are required (Blatter & Haverland, 2012, p. 82). Seeing how both countries have been developing their cybersecurity approaches for a relatively long period of time, a multitude of research and policy reports, parliamentary proceedings, strategies and such are available for analysis.[3]

More significant than this practical consideration, however, is the relative weight of both countries in terms of cybersecurity proficiency. Whereas the Netherlands ranks fifth the ITU's Global Cybersecurity Index (GCI), France is ranked second within the Europe region (ITU, 2017, p. 56). Moreover, both countries are cited as advanced cybersecurity actors in the European context (Carrapico & Barrinha, 2017, p. 1264; Robinson, 2014, p. 2). The United Kingdom constitutes another such member state, but given the wide availability of English language sources, its cybersecurity policies have been the subject of several similar research projects before (cf. Carr, 2016; Christou, 2016; Coaffee & Fussey, 2015; Herrington & Aldrich, 2013). Moreover, due its withdrawal from the European Union, researching how UK policies relate to the European context becomes more problematic.

Cases with a more advanced cybersecurity approach, such as the Netherlands and France, are more likely to adopt a type 3 resilience as security approach, given the amount of features of this strategy that have been recognised as crucial for effective cybersecurity policy in the academic literature. As Blatter and Haveland (2012a, p. 104) propose, for research concerned with explaining outcomes, case selection can take place based on similarity of outcomes, with different pathways leading to that outcome. As two countries with similar cybersecurity proficiencies and vastly different institutional settings, France and the Netherlands as units of analysis are likely to provide insight into the causal mechanisms that explain the respective logics underlying their cybersecurity approach.

Data collection and generalisability of research results

The principle form of data that this research relies on is documentation, in the form of policy papers, research institution reports, ENISA and government reports, parliamentary proceedings, academic research and, occasionally, news reports and publications. In addition, blog posts by

[3] Both France and the Netherlands published their first national cybersecurity strategies as early as 2011.

academic authors are occasionally used to provide context. Relying on documentary evidence, however, is not without its weaknesses. Although it allows for analysing processes over a longer time span with relatively stable evidence, access and a selective bias present two difficulties (Yin, 1998, p. 231). Perfect access and a complete absence of bias are unfortunately unattainable, but effort can be made to counter these obstacles. Although access, especially for information relating to actors' motivation is difficult, motives can be inferred by combining information on discourse and empirical information of actions carried out (Blatter & Haverland, 2012, p. 117). Bias can be countered through careful and thorough collection of evidence and the creation of a case study database on the different policy areas of cybersecurity under analysis in order to efficiently and structurally organise data (Yin, 1998, p. 248). This aids in identifying gaps in the knowledge and provides a method of structuring counterfactual evidence.

Generalisability for small-*n* case studies employing causal-process tracing does not refer to statistical generalisation, i.e. drawing conclusions that apply to cases with similar independent variables (Blatter & Haverland, 2012, p. 135). Instead, the goal of this research is to explain how and why an outcome, the type of resilience as security in cyberspace, has come about in the case of France and the Netherlands. Findings from such analysis are especially relevant for theoretical purposes, by testing the usefulness of the resilience framework for cybersecurity policy analysis. Moreover, through this theoretical framework, the thesis aims to provide an in-depth understanding of the conceptualisation of resilience within the cybersecurity approaches of two leading EU member states. Should the outcome not be a type-3 resilience, or a mixture of logics, explaining how this has come about provides guidance for further analysis of the cybersecurity approaches in different states.

The Netherlands: an adaptable ecosystem with diffused responsibilities

In the European context, the Netherlands is one of the continent's most well-connected countries. According to an analysis of Eurostat numbers by Statistics Netherlands (CBS), the government agency gathering statistical data, the country has the highest rate of internet penetration at 98% of the population, an 86% rate of mobile internet users, as opposed to a European average of 69%, and 80% of its citizens indicated they have made online purchases (CBS, 2019, pp. 71–73). Its top-level domain extension, .nl, is the eight-most used globally, making it only slightly more popular than Russia's .ru (DomainTools, 2019). Since a first introduction to the internet through a bulletin board-style USENET in 1982 and the establishment of connectivity with the US in 1988, the Netherlands has evolved into a European internet gateway. It hosts the Amsterdam Internet Exchange (AMS-IX), currently one of the largest such exchanges worldwide, connecting over 800 communication networks spread across five continents (AMS-IX, 2019).

Internet and connectivity matter to the Dutch economy as well. It is a top-ten exporter of internet goods and services, and the information communications and technology (ICT) sector accounts for roughly 5% of national GDP (Rademaker et al., 2016). Nonetheless, this connectivity is accompanied by risks. 73% of companies with more than 500 employees faced an ICT-related security incident in 2016, over half of which resulted in additional costs for the organisation (CBS, 2018, pp. 30–31). Moreover, one out of nine citizens fell victim to cybercrime at least once in 2017 (CBS, 2018, p. 36). Such cybercrimes include identity theft, hacking into personal websites or email accounts and cyber bullying. Since 2011, with the publishing of its first Digital Agenda and National Cybersecurity Strategy, the Dutch government has recognised the growing importance of its digital economy and the risks accompanied by an increasing reliance on ICT. Since then, it has moved towards creating a more flexible cybersecurity ecosystem with a variety of responsible stakeholders. With a coordinated approach to the private sector and new institutional structures, the Netherlands is moving towards a type-3 classification of its cybersecurity system, despite a relative lack of structural funding indicating a prolonged focus on efficiency in governance logics rather than redundancy.

The analysis of the Dutch cybersecurity landscape as laid out in national strategic documents and reviews is the main focus of this chapter. By characterising the Netherlands' cybersecurity approach and discussing the extent to which it adheres to the conditions for achieving resilience in cyberspace, as well as breaking down the evolving narrative, important conclusions can be drawn about its good (and possibly not so good) practices within a European

context. After outlining the evolving national cybersecurity landscape and the logics underpinning its development, the research focuses on similar developments in the fields of cyberdefence and combating cybercrime.

National strategy: from awareness to capability to consolidation

In 2011, the Dutch government introduced its first national cybersecurity strategy titled 'Strength through cooperation' (Ministry of Security and Justice, 2011) after being spurred to do so by parliament, which noted an absence of funding for cyberwarfare in the defence budget and asked the government to develop a cybersecurity strategy (Knops, 2009). The strategy is stooled on the dual logic of promoting economic growth by becoming 'the Digital Gateway to Europe' while simultaneously recognising new vulnerabilities stemming from an increased reliance on complex ICT systems (Ministry of Security and Justice, 2011, p. 3). Tying together economic and national security concerns, the strategy aims to facilitate a safe and reliable open digital society (Ibid., p. 7). Stated priorities are to create an integrated public-private approach; to enhance resilience against disruptions; to increase operational capabilities; to intensify the investigation of cybercrimes and to promote further research and education concerning cybersecurity (Ministry of Security and Justice, 2011, p. 8).

Notably, the strategy identifies an incoherence between existing policies and operational capabilities and seeks to create new basic operating assumptions and institutional structures. It aims to facilitate a more network-centred mode of public-private cooperation by establishing a Cyber Security Council (CSR), an independent advisory body including representatives from the private and public sector as well as from academia. The CSR, which became operational in 2011, is tasked with providing strategic advice to government and with raising awareness of strategic cybersecurity issues in the private sector (CSR, 2020). In tandem with the CSR, the strategy proposes the establishment of a National Cyber Security Centre (NCSC) to serve as a nodal platform for cooperation between public and private parties. Under the auspices of the Ministry of Justice and Security, the NCSC is tasked with national incident response, information exchange and the promotion of cooperation. The NCSC became operational in January of 2012. Moreover, among other cybersecurity-related publications, it publishes the annual Cyber Security Assessment Netherlands with the goal of fostering a common understanding of threats and vulnerabilities.

The first strategy places strong emphasis on individual responsibility, including that of businesses, individuals and public institutions (Ministry of Security and Justice, 2011, p. 6). In a similar vein, it emphasises self-regulation over legislation wherever possible. To this end, the

strategy, noting the large proportion of ICT infrastructure and services provided for by the private sector, speaks repeatedly of the value of coalitions of public and private actors working in partnerships, such as a pool of public and private experts to share expertise on cybercrime (Ministry of Security and Justice, 2011, p. 13). It recognises that building mutual trust is essential to the well-functioning of these partnerships.

Whereas the strategy seeks to raise awareness about cybersecurity issues and demonstrates a willingness to adopt new institutions and operating assumptions, such as linking existing initiatives, it does not yet display a full commitment to abandoning assumptions of efficiency. Saliently, it states that all the mentioned action lines "will be absorbed within existing budgets." (Ministry of Security and Justice, 2011, p. 15). This stands in stark contrast to the UK, for example, which allocated £650 million in cybersecurity funding for a four-year period in its 2011 strategy (Cabinet Office, 2011, p. 6). Although the strategy displays the need for increased coherence and efficiency in national cybersecurity policy, it still lacks the urgency to fully implement an approach that could be said to lead to type 3 resilience as security in cyberspace.

With the publication of its second national security strategy in 2014, the Dutch government takes a broader and more far-reaching approach to the provision of cybersecurity. The strategy, titled "From awareness to capability", was drafted in cooperation with a wide range of actors from public and private institutions, as well as academia and social organisations (Ministry of Security and Justice, 2014, p. 3). Its stated ambitions are to increase resilience to cyberattacks and to protects vital interests; to tackle cybercrime; to provide secure ICT services; to build international coalitions to further freedom and security in the digital domain; and to have sufficient cybersecurity professionals and skills (Ministry of Security and Justice, 2014, p. 8).

An important aspect of the new strategy is the more central position of the NCSC in the cybersecurity landscape. In addition to its role as an emergency response centre, the NCSC is elevated to the expert authority in the field of cybersecurity, advising both public and private parties. This coincides with a pointedly different role envisioned for the government, shifting focus away from individual responsibility to a more guiding government that sets standards and can determine regulations wherever necessary in consultation with relevant private actors (Ministry of Security and Justice, 2014, p. 19). (Self) regulation mentioned in the strategy includes developing concepts such as the 'duty of care' that providers of ICT networks and services should have towards their customers, hereby increasing the convergence amongst stakeholders on common norms and standards of security in cyberspace.

Another domain in which the Dutch government in the second strategy strives towards a common understanding of norms and standards is on the international level. It aims to take a leadership position in international cooperation in respect to capability-building, while protecting fundamental rights and values in line with the European Cybersecurity Strategy (Ministry of Security and Justice, 2014, p. 14). Measures in this domain include promoting the ratification of the Budapest Convention on Cybercrime, which aims to harmonise criminal law on cyber-related offences, and co-founding the Freedom Online Coalition, a multi-stakeholder lobbying organisation with over 30 member states that promotes internet freedom and human rights online (Hathaway & Spidalieri, 2017, p. 34).

The revised strategy aims to create a more structural approach to public-private partnerships. Whereas the 2011 strategy proposed several such partnerships, including the NCSC and a partnership on cybersecurity research and education, the 2014 document aims to consolidate these efforts, mainly in the field of information-sharing. Examples of these include a national detection and response network for the central government and providers of vital services, to share threat information on the basis of trust and confidentiality (Ministry of Security and Justice, 2014, pp. 23–24), and the development of cyberdefence training for the military in cooperation with private parties (Ibid., p. 33). Such public-private partnerships also serve to promote awareness on cybersecurity-related issues.

The evolution of a culture of cybersecurity on all levels is promoted through the whole-of-nation approach embodied in the NCSS2, which is perhaps the clearest distinction between the two strategies. Instead of treating cybersecurity as a more technical security issue, the strategy regards cybersecurity as connected to wide range of other policy areas including diplomacy, human rights, social-economic benefits and internet freedom (Ministry of Security and Justice, 2014, p. 3). Moreover, it seeks to increase the digital resilience of the government, individual citizens and the private sector by promoting 'basic cyber hygiene' through awareness campaigns, investing in digital skills and research as well as by supporting social organisations (Ministry of Security and Justice, 2014, p. 20).

In the second NCSS, over twenty different organisations or organisation types are referred to as responsible for one or more parts of cybersecurity policy (Ministry of Security and Justice, 2014, p. 28). These include General Intelligence and Security Service (AIVD) and its military counterpart, the MIVD, as well as the Ministry of Defence (MoD), police services and the private sector. In the absence of a central office coordinating cybersecurity developments, success is dependent on the outcomes of consensus-seeking cooperation and negotiation between the different actors. This so-called *polder* model is widely recognised as a characteristic

feature in Dutch cybersecurity policy (Boeke, 2016, p. 7; Broeders, 2014, p. 30; Clark et al., 2014, p. 30; Hathaway & Spidalieri, 2017, p. 6). As an organisational model, it could foster an integrated approach between various different parties, but it could also hamper and stall decision-making procedures if parties disagree strongly. Furthermore, the strategy again does not provide for additional funding, stating that its outlined action programme is to be executed within the scope of existing ministerial budgets or partner budgets (Ministry of Security and Justice, 2014, p. 26). This means that the strategy still does not create funding with space for redundancy, holding on to assumptions of efficiency rather than complexity in governance logics.

In its third and current national strategy of 2018, named the National Cyber Security Agenda (NCSA), the Dutch government does allocate additional structural funding of €95 million, to be used for increasing staff capacity and the expansion of ICT facilities (Ministry of Security and Justice, 2018, p. 17). Its main objective is to make "the Netherlands capable of capitalizing on the economic and social opportunities of digitalisation in a secure way and of protecting national security in the digital domain." (Ministry of Security and Justice, 2018, p. 7). The NCSA favours an integrated approach to cybersecurity with increased coordination from the government side (Ministry of Security and Justice, 2018, p. 43). Rather than simply becoming a digital gateway to Europe, the NCSA ambitiously states the desire to become a leader in the field of cybersecurity knowledge development as well as in developing digitally secure hardware and software.

In terms of coalitions of public and private actors working on the basis of trust to share information, the NCSA, which regards this as the basis for the Dutch cybersecurity approach, notes that this cooperation has improved greatly in recent years (Ministry of Security and Justice, 2018, p. 19). Nonetheless, it goes on to say that existing cooperation and information-sharing should be more structurally guaranteed, by for example coordinating roundtable discussions under auspices of the National Counter-Terrorism and Security Coordinator (NCTV) or by having the NCSC develop cybersecurity partnerships concerning basic security measures. Such partnerships include the Information Sharing and Analysis Centres or ISACs, of which at least 17 known varieties exist, each centred on a sector such as finance, water management or energy provision (Verhagen, 2016, p. 26).

Creating convergence among stakeholders on common standards of security as resilience is another major ambition of the NCSA, most notably through the development of standardisation and certification initiatives both domestically and internationally (Ministry of Security and Justice, 2018, p. 27). The Netherlands was a strong advocate of the European

Cybersecurity Act, which, among others, established a common European certification scheme. Another means to further convergence is the discussion on when an ICT supplier is liable for insecure hardware or software. In other international fora, the Netherlands advocates confidence-building measures between states and the development of international norms applicable in cyberspace (Ministry of Security and Justice, 2018, p. 23).

The NCSA emphasises the aspiration for the "mainstreaming of cybersecurity", iterating that it must be part of everyday processes in every organisation (Ministry of Security and Justice, 2018, p. 7). To this end, the Dutch government has launched several awareness campaigns such as the *Eerst checken, dan klikken* [check before you click] campaign in 2019 or via efforts by the Alert Online group, a coalition of public and private actors founded by the NCTV to promote awareness of cyber hygiene among all sections of Dutch society (Alert Online, 2020). Alert Online also publishes an annual cybersecurity awareness monitor with recommendations for future campaigns, indicating attention to structural learning in the development of these campaigns (Bot & Hengstz, 2019).

Over the course of eight years, the Dutch government has markedly widened the scope of its national cybersecurity strategy, by linking its security policies to human rights and social-economic benefits as well as recognising that a culture of cybersecurity is necessary at every level in society. In setting up the CSR, NCSR and several other platforms for public-private cooperation and by trying to create more structured means of cooperation, the strategies display the ability and preparedness to adopt new operating assumptions and institutions. Especially with the NCSA, the Dutch government has made strong efforts to standardise ICT standards and to develop norms in (international) cyberspace.

Despite these strongpoints of the Dutch national strategy, two main deficiencies in the Dutch approach can be identified. The first is the lack of budgetary government funding, notably in the first two strategies and to a lesser extent in the NCSA. Not only does this stand in contrast to the discourse prioritising cybersecurity as part of national security provision, the lack of space for redundancy in the capacity to mitigate threats could harm the overall resilience of the Dutch cybersecurity system. Secondly, although it has not led to major problems or inefficiencies, the large amount of actors with diffuse responsibilities in the cybersecurity landscape could stagger decision-making in times of crisis.

Centralised responsibility and reliance on third parties in cyberdefence

On the basis of the first national cybersecurity strategy, the Dutch Ministry of Defence (MoD) published its 'Defence Cyber Strategy' in 2012 (Ministry of Defence, 2012) which was

subsequently updated in 2015 and in 2018. It recognises cyberspace as the fifth domain for military operations, alongside air, sea, land and space. Underlining both the risk that vulnerabilities in cyberspace pose as well as the potential these vulnerabilities can provide for military operations, the strategy is explicit about developing defensive *and* offensive capabilities (Ministry of Defence, 2012, p. 5).

Other structures provided for by the Defence Cyber Strategy are the Joint Information Management Command (JIVC) and the establishment of a joint SIGINT-Cyber Unit (JSCU) of the AIVD and MIVD (Ministry of Defence, 2012, p. 12). JIVC is responsible for the protection and monitoring of military networks and as such includes the DefCERT. As for the JSCU, it is the platform in which both intelligence services share their signals and cybercapabilities. Since these organisations employ different ICT infrastructures, there have been some issues with the varying levels of capacity, especially that of the MIVD (CTIVD, 2019, p. 16).

The strategy is stooled on the understanding that operating in cyberspace requires new operating assumptions such as rapidly implementing new technologies and a constant readjustment of working methods (Ministry of Defence, 2012, p. 5). To this end, it foresees in the establishment of a Defence Cyber Command (DCC), which became operational in 2014. The DCC is responsible for the coordination of all tasks relating to cybercapacities within all services of the military. Moreover, it oversees several forms of operations including cyberintelligence, supporting missions, combat operations and passive measures that can be applied to all categories of military missions (Hathaway & Spidalieri, 2017, pp. 37–38). Whenever required, mission teams from the DCC can include members of the military intelligence services, given how similar the tools required for military and intelligence operations are in cyberspace (Ministry of Defence, 2018a, p. 13).

Although the ambition of the MoD is to strengthen its own knowledge position in order to become less dependent on third party expertise (Ministry of Defence, 2018a, p. 15), it acknowledges that partnerships with private and academic actors are essential to the provision of cybersecurity. Examples of these include the strategic cryptography partnership with the company FoxIT (Ministry of Defence, 2018a, p. 16) or the education programme that military personnel has followed with the same organisation (Pelk, 2017). In addition to this limited cooperation with private actors, the Dutch government actively pursues the operationalisation of the digital domain within the NATO, which is regarded as a cornerstone of Dutch security policy. Furthermore, the Netherlands has organised cross-border cybersecurity exercises with Germany (Ministry of Security and Justice, 2012) and has participated in the ENISA Cyber Europe exercises (ENISA, 2018).

In order to increase the awareness of cybersecurity issues within the ministry, digital and cybersecurity-related aspects of every potential mission are to be considered in the early planning stages (Ministry of Defence, 2018a, p. 13). This includes informing the Dutch parliament as much as possible about the contribution made to any potential mission through the use of cybercapabilities. Although the exact allocation of MoD budgets is classified, the Dutch government has apportioned up to €48 million for the development of cybercapabilities from 2018 to 2021, with a structural funding of €20 million annually after 2021 (Ministry of Defence, 2018b, p. 27). Moreover, it has allocated almost €1.5 billion for ICT-related investments (Ibid.). According to some, the budget for the development of cyber capabilities remains far below of what would be required (Boeke, 2018; Smeets, 2018). As of 2018, the DCC had not yet undertaken any offensive actions or received a political request to do so (Van Lonkhuyzen & Versteegh, 2018).

The Netherlands has managed to create a clear structural division of responsibilities in the realm of cyberdefence, with the DCC in charge of mission-related operational aspects and the JIVC tasked with the defence of the MoD's own networks. It has recognised the importance of developing an own knowledge base, while also cooperating with the private sector, albeit in a limited capacity. Through involving cybersecurity aspects in every part of planning processes, the MoD has sought to increase the awareness of cybersecurity throughout the organisation. However, as with the national strategies, the defence cyberstrategy also demonstrates a shortage of funding which will likely entail a continued reliance on private sector actors for the provision of certain parts of its cybersecurity system.

Tackling cybercrime: from obscurity to a culture of cybersecurity

As mentioned in the introduction of this section, the Netherlands knows a high volume of cybercrime, partially due to its well-connected society. Internationally, the Dutch government has committed itself to protecting society against cross-border cybercrime through ratifying the Budapest Convention in 2006, the Council of Europe convention against cybercrime, as well as through cooperating with Europol's Cybercrime Centre which has its headquarters at the Europol offices in The Hague. Moreover, it has domestically introduced and updated laws to counter cybercrime, such as the Computer Crime Act of 2018, and to enforce data protection through the European General Data Protection Regulation, which supplanted existing national laws.

Since 2008, the Dutch police has sought to enhance its capabilities to combat cybercrime with the 'Programme Cybercrime Approach' which led to the establishment of a national

helpdesk for internet fraud (Boekhoorn, 2019, p. 13). Responsibility for tackling cybercrime is divided over different organisational levels. Team High Tech Crime (THTC), formed in 2007, is responsible for nation-wide and international cybercrime cases, whereas regional units, started in 2015, are responsible for countering other forms of cybercrime (Van Bree et al., 2016, p. 9). Eight out of ten regional organisations now have such 'cyber units', although their capacity and expertise varies widely from region to region, hindering their capacity for doing research together (Boekhoorn, 2019, p. 23). THTC has booked some international success, including infiltrating and stopping a dark web market named Hansa (Van Lonkhuyzen & Meeus, 2017) and halting the work of the largest website providing DDoS-attacks (Politie.nl, 2018). Thanks to these achievements, the THTC enjoys an international reputation as an effective cyberpolice unit (Boekhoorn, 2019, p. 34).

An important pillar of the cybercrime approach is prevention, with additional attention to those groups that are considered digitally vulnerable (*Kamerbrief Integrale Aanpak Cybercrime*, 2018, p. 5). An example of this is the No More Ransom project, a public-private cooperation between the Netherlands National Police, Europol and private actors that focuses on the prevention and mitigation of ransomware attacks. Another is the establishment of the Digital Trust Centre, a government agency aimed at improving the cyber resilience of small and medium-sized businesses (Digital Trust Center, n.d.). These measures are aimed at lowering the frequency of cyberattacks through enhancing the resilience of Dutch society.

One challenge for the Dutch police is to improve the intake and reporting of cybercrime, as those reporting the crime often do not feel recognised by the police authorities (Van Bree et al., 2016, p. 2). Although the police cyberteams have raised awareness for cybercrime reporting in the intake department, the relative obscurity of cybercrime and digitalised criminality still proves to be a hindrance to proper intake and reporting (Boekhoorn, 2019, p. 60). Reporting statistics for cybercrime are already low in comparison to other forms of crime (CBS, 2018, p. 37) and as of October 2019, it is not yet possible to declare cybercrime online, with the exception of internet fraud. In order to improve the intake percentage, more effort should be made to create awareness of cybercrime in all layers of the police organisation.

An open and flexible cybersecurity ecosystem moving towards maturity

Since the introduction of the Internet in the 1980s, the Netherlands quickly became one of the most digitalised countries on the European continent with a substantial ICT industry. From aiming to raise awareness about cybersecurity issues in its first NCSS of 2011, the Netherlands has shifted focus towards capability building in 2015 and towards the consolidation and

mainstreaming of cybersecurity policies in 2018. Although the Dutch cybersecurity ecosystem relies on a diffuse network of actors and institutions for implementation and has only recently been structurally funded, there are strong indicators that the Netherlands is moving towards an 'Openness and Adaptability' type-3 approach of achieving resilience, while retaining some 'Change at the Margins' type-2 approaches in its national strategy, mainly because of its focus on efficiency in governance logics.

Having identified an incoherence between existing policies and capabilities, the government introduced two new institutions as central nodes in the institutional cybersecurity network, the CSR and the NCSC. Both are public-private partnerships under the auspices of the Ministry of Justice and Security. Whereas the national strategies initially emphasised individual responsibility of end users and private entities, the onus to create coherence and common standards shifted to the government in later strategies. Instead of self-regulation, the state took a more active approach in setting standards and co-creating regulations where necessary. This approach underlines the importance attached to achieving cybersecurity objectives in trust-based cooperation with the private sector, a cornerstone of the Dutch strategies.

Particularly after the NCSA, the Dutch government has taken an active approach to setting norms and standards in cyberspace, both through international cooperation in different fora as well as through certification schemes on the European level. Concurrent with furthering convergence on these issues are the efforts to involve cybersecurity questions and efforts at every level of government policy and decision-making, such as considering digital aspects in every military planning operation or in all police units. In combination with several awareness-raising projects, aimed at both government actors as well as individual citizens, the Netherlands is on its way to creating a cybersecurity culture at all levels among stakeholders. Although the ecosystem relies on a wide variety of responsible actors, resulting in different capacity levels among police units for example, a more integrated approach can be witnessed in the whole-of-nation approach to national strategy and the clear division of responsibilities in cyberdefence.

France: centralised guidance and shared governance

On the Digital Economy and Society Index, a monitor of EU member states' digital progress published by the European Commission, France ranks 15th with a score slightly below the European average (European Commission, 2020a, p. 3). The index tracks progress in the areas of connectivity, human capital, use of internet serves, digital public services and the integration of digital technology. Despite its ranking below the European average, France has the highest number of employed ICT specialists after Germany and the UK, as well the largest expenditure on research and development with €7.7 billion, making up 23% of the total European spending on R&D (European Commission, 2020b, pp. 54, 111).

France is a well-connected European country, boasting fixed broadband take-up among 73% of households, near-universal 4G coverage and 96 mobile broadband subscriptions per 100 people (European Commission, 2020a, p. 6). Whereas the difference in uptake between rural and urbanised areas is practically non-existent in the Netherlands, France still has a relatively low rural uptake of fixed broadband connections with a rate of 63% (p. 28), meaning it still has some way to go to providing universal internet access. Through its *grand plan d'investissement*, a €57 billion public investment programme launched by the government in 2017, France hopes to encourage private sector innovation in areas such as cybersecurity, big data use and artificial intelligence research (Philippe, 2017).

Such large-scale investment projects are not new to French digitalisation efforts. In 1981, a unique national service called Minitel was introduced to French citizens by the state-owned national telecommunications provider France Telecom. This text-based modem service, subsidised by the French government, allowed users to chat, bank, make reservations and to purchase items 'online'. The main rationale behind the Minitel project was to create a digital society in France and to facilitate a French technological independence. Eclipsed, however, by the introduction of the worldwide web, the Minitel service was retired in 2012. It can be seen as a prime example of the French model of state-led innovation growth, with the government actively shaping conditions for the private sector to work in.

This chapter focuses on the analysis of the French cybersecurity ecosystem, as laid out in several national strategies and strategic reviews. By benchmarking the characteristics of the French system against the criteria for achieving effective resilience in cyberspace and by discussing the evolution the cybersecurity narrative has followed in France, conclusions can be drawn concerning the typology of the French system. From the strongly centralised, state-led and sovereignty-focused initial strategies, France has developed a more flexible orientation

involving a wide variety of private actors and with a dedication to establishing common norms and standards in cyberspace. Despite its move towards a type-3 'Openness and Adaptability' ecosystem, France has retained some of its centralist policy guidance as well as a more regulatory approach to cybersecurity issues than the Netherlands. After outlining the French national strategies and white papers, the chapter discusses the French approaches to military cyberdefence and combating cybercrime.

French national strategy: protecting sovereign and fundamental interests

Nationally, the progress towards dealing with cybersecurity on a strategic level was launched in 2008, when President Sarkozy called for a wide-ranging review of the national security and defence strategy. This resulted in the 2008 White Paper on Defence and National Security, which recognised cyberattacks as a new threat and prioritised the coordination of defence against such attacks (Sarkozy, 2008, pp. 7–8). Noting that cyber war would be a major concern for France, the White Paper proposes to coordinate cybersecurity efforts by a new Security of Information Systems Agency, which was launched in 2009 under the name *Agence nationale de la sécurité des systèmes d'information* (ANSSI), and expresses the desire to develop offensive cyber war capabilities (Sarkozy, 2008, p. 12). ANSSI is tasked with implementing a preventive and reactive policy in defence against cyberattacks under the auspices of the General Secretariat for Defence and National Security (SGSDN), coordinated by the Prime Minister.

In addition to prioritising the coordination of cybersecurity capabilities, the document also identifies several areas of industry over which France should retain its sovereignty in order to maintain the strategic and political autonomy of the state. Alongside nuclear deterrence, ballistic missiles and nuclear submarines, cybersecurity is regarded as an industrial area imperative to retaining sovereignty (Sarkozy, 2008, p. 10). Such a focus on supporting and retaining an area of industry fits into the French tradition of providing large amounts of public aid to military industry, but also of providing aid to national information and communication technology industries (D'Elia, 2018, p. 387). This state-led public innovation is exemplified by the Minitel service and the deployment of a national optical fibre network. Guaranteeing national independence and sovereignty by promoting large-scale public projects of technological excellence is characterised as a trait of the French approach, defined as 'high-tech Colbertism' (Sachwald, 1997, p. 15). However, the method of pursuing this approach has markedly differed from the time of Minitel, given that private corporations are the main providers of cybersecurity-related products. This means that public-private cooperation is essential in reaching the goals of the White Paper.

One of the more tangible results of the 2008 White Paper was the establishment of ANSSI. It is tasked with advising the government on cybersecurity-related efforts, as well as assisting operators of critical infrastructure (OIV) with enhancing their cybersecurity efforts (Baumard, 2017, p. 57). In addition to this, it houses the CERT-FR and is designated as the national authority for the defence of government information networks. ANSSI has since seen its initial budget grow from €43 million in 2014 to over €100 million in 2018 and it aims to reach 675 members of staff in 2022 (Regards Citoyen, 2018). Notably, the 2014-2019 Military Planning Law authorised ANSSI to set compulsory rules for OIV security systems and to hold security inspections when deemed necessary (Hathaway et al., 2016, p. 9). This stands in contrast to the NCSC in the Netherlands, which does not possess a similar degree of regulatory clout, emphasising coordinated regulation instead.

Besides its regulatory and advisory functions, ANSSI was tasked with drafting a national cybersecurity strategy for France in 2011, released shortly after a cyberattack targeted the core systems of the ministries of finance and economics (Valls, 2015, p. 7). This strategy became the 'Information systems defence and security: France's strategy', outlining the steps France has taken since the White Paper was published (ANSSI, 2011). The document outlines four strategic objectives for the cybersecurity policy of France, namely to become a world power in cyberdefence; to safeguard national decision-making ability; strengthening the cybersecurity of critical national infrastructure and to ensure security in cyberspace.[4] In correspondence with the White Paper, the cybersecurity strategy is strongly stooled on the logics of protection of national sovereignty and maintaining the strategic independence of France.

Although the first cybersecurity strategy proposes areas for public-private cooperation, such as the establishment of a research centre with industrial partners and the need to strengthen and scale technological industries through state resources (ANSSI, 2011, p. 16), PPPs are not as centrally posited as in the first Dutch NCSS. In addition to proposing a public-private research centre, the strategy also recommends a partnership with operators of critical infrastructure, in order to let operators benefit from state-gathered threat analysis and to "allow the State to ensure the appropriate level of protection of the infrastructures that are crucial to keep the country running properly." (ANSSI, 2011, p. 17). In this case, as well as with the strengthening of the industrial base, governance appears to be highly state-led rather than dispersed between

[4] Cyberdefence in France refers to the entire national framework ensuring the protection of state networks, including those of the Ministry of the Armed Forces. Responsibility for cyberdefence is therefore placed with ANSSI, with the ministry exclusively responsible for its own networks (Delerue et al., 2019). Military cyberdefence is thus used here to refer to the latter.

actors and sectors. Moreover, the document does not mention if these partnerships would be voluntary or trust-based.

In regard to creating convergence among stakeholders on a 'common' understanding, the strategy does recognise the need for legislative and regulatory frameworks to reflect the development of cyberspace (ANSSI, 2011, p. 18) so as to diminish the threat these could pose to individual freedoms. However, the strategy does not mention norms or values such as guaranteeing an open internet or human rights in cyberspace as drivers for France's policy. It does state raising awareness of cybersecurity issues during education as a long-term objective, as well as the desire to ensure awareness of these issues in all layers of society through communication campaigns (ANSSI, 2011, pp. 18–19).

In 2013, President Hollande called for another strategic review of defence and national security, resulting in the 2013 French White Paper (Hollande, 2013). Again, the possibility of a major cyberattack on national information systems is identified as a serious threat with the potential to undermine the sovereignty of France. To counter this threat, the report notes the necessity of substantially increasing the level of security and the means to defend information systems, among others by reinforcing human resources dedicated to cybersecurity on a scale similar to that of Germany or the United Kingdom (Hollande, 2013, p. 100). In line with the 2011 strategy, preservation of national and European industries for high-level security systems is marked as an essential objective. Moreover, it is the state that defines cybersecurity standards for operators of vital importance, with ANSSI having the responsibility for intervening in the event of a serious crisis (Hollande, 2013, p. 101).

After the publication of the 2013 White Paper, Prime Minister Valls engaged in consultation with a large variety of stakeholders, including the private sector and the ministries of defence, the interior and foreign affairs, resulting in the 2015 national cybersecurity strategy called the 'French National Digital Security Strategy' (Baumard, 2017, pp. 60–61). In a few remarkable ways, the strategy differs from its 2013 predecessor, most notably by departing from focussing on protection of sovereignty to the protection of 'fundamental interests', a wider conceptualisation that encompasses operators of vital importance, military operations and guaranteeing public debate (Valls, 2015, p. 14). Besides the protection of fundamental interests in cyberspace, promoting digital trust and combating cybermalevolence, raising awareness and continuing education, promoting digital industry and achieving (European)

digital strategic autonomy are the main objectives of the second NCSS.[5] Strikingly, the second strategy identifies private monopolies in cyberspace as a threat owing to the monopolising of digital data and the dependency this creates for other actors (Valls, 2015, p. 38).

In contrast to the first strategy, public-private partnership takes a more central role in achieving the stated goals. Private stakeholders are regarded as crucial actors for reinforcing the security of critical networks, although the strategy does not outline exactly what type of partnerships are desired (Valls, 2015, p. 3). In regard to providing assistance to victims of cybermalevolent acts, however, the document does propose a PPP with a legal form to aid victims to find support from local stakeholders and to encourage the lodging of complaints (Valls, 2015, p. 21). It is supported by regional networks of ANSSI, software editors and digital solution providers. Despite these various integrated public-private approaches, support of the cybersecurity industry by the state, through fund-raising as well as through international promotion, still takes a central role in the strategy of France (Valls, 2015, p. 34). These support efforts are directed through the 'Industry of the Future' plan, putting forward industrial policy designed in cooperation with private stakeholders and guided by the government, oriented towards promoting excellence in the development of digital technologies (European Commission, 2017).

Markedly, the 2015 strategy takes a more normative turn by categorising the role of the state in cyberspace as promoting France's values and as guaranteeing freedom of expression and action (Valls, 2015, p. 9). Individual rights should apply both in the 'online' and 'offline' worlds and France advocates for preserving a free and open cyberspace (p. 21). Moreover, universalising and consolidating the norms of the Budapest Convention is stated as another objective. These statements mark a more explicit shift towards normative convergence in comparison to the 2011 strategy. In addition to normative convergence, the government aims for convergence on standards of security as well, such as with the State Information Systems Security Policy (PSSIE), an inter-ministerial cybersecurity policy aimed at safeguarding decision-making procedures (Valls, 2015, p. 15). Finally, the strategy extends the 2013 White Paper goal of achieving strategic autonomy to the desire to realise a European digital strategic autonomy in terms of regulation, standardisation, trust and research (p. 39). France can thus be seen as taking a more active role, both nationally and internationally, in an attempt to create convergence on norms, security standards, laws and logics.

[5] The term 'cybermalevolence' in the strategy refers to acts that constitute cybercrime and those that threaten the digital privacy of citizens.

Comparing itself to its 'partners', the strategy notes that France is late in raising awareness of the risks associated with using digital technologies and that, in general, its population neglects good practices (Valls, 2015, p. 26). To this end, the policy focus lies strongly on increasing educational efforts for young citizens, such as through the "A digital education for all" programme of the National Commission on Informatics and Liberty (CNIL) (CNIL, n.d.). Furthermore, cybersecurity awareness is to be incorporated into all higher education programmes with the cooperation of higher education interest organisations. Attempting to create a culture of cybersecurity on the regulatory level as well, the strategy recognises the need of monitoring emerging technologies in order to continuously adapt the regulatory framework. In doing so, the strategy emphasis the necessity of 'learning to learn' in the creation of rules.

Subsequently, in 2018 the SGDSN published the first Strategic Review of Cyber Defence, a multi-stakeholder reassessment for improving the cybersecurity efforts of France and for improving cybersecurity in French society (SGDSN, 2018). The white paper is divided into three parts: identification of risks, including the extraterritoriality of data and the strong influence of US-based firms over these data, the role of the state in cybersecurity and the role of the state in societal cybersecurity. In conceptualising the French model of cybersecurity, the review notes that its approach lacked a clear outlining of governance mechanisms, core principles and a clarification of its operational organisation (SGDSN, 2018, p. 5). To strengthen governance, a Cyber Defence Management Committee is established, tasked with monitoring and evaluating policy decisions on the organisation and development of the cyberdefence area. Moreover, it proposes the creation of an inter-ministerial cybercrisis coordination centre to facilitate governmental responses to these attacks (p. 6). These new institutional structures and clarified operating assumptions point to the development of a clear coordination for responsibilities related to the provision of cybersecurity.

Prominently, the document sets out the French notions on the applicability of international law in cyberspace and argues that the state should endeavour to universalise such conceptions in order to strengthen international cooperation (SGDSN, 2018, p. 9). These include efforts to establish a mechanism for joint crisis management and de-escalation, as well as defining principles under which states targeted by cyberattacks can take appropriate measures in retaliation. With its strong commitment to the use of international law and the explication of its perspective on international norms, this document is likely one of the most comprehensive statements on the use of international law ever published by the French government (Delerue & Géry, 2018). Moreover, by putting forward a scale of potential responses to cyberincidents loosely based on the US Cyber Incident Severity Schema, the white paper gives a predefined

set of military and non-military responses to French leadership in order to guide their actions (Toucas, 2018).

The 2018 strategic review is a wide-ranging initiative aimed at formulating a cyberwarfare doctrine for France, based on consolidating its institutional structure and operating assumptions. Moreover, it is an attempt at facilitating convergence on international norms and coordinating an integrated approach to cyberincidents. It marks a clear evolution from the language of the 2008 White Paper, which was focused on setting up rather than consolidating national cyberdefence. By publicly setting out its doctrine, France has been said to assume the posture of a global cyber power (Delerue et al., 2019). Through strengthening governance mechanisms and by clarifying its stance on international norms, France is moving towards an open and adaptable cybersecurity system.

Becoming a world player in military cyberdefence

After the terrorist attacks on the French satirical newspaper *Charlie Hebdo* in 2015, several French websites, including those of the Ministry of Defence, fell victim to cyberattacks from activists linked to Islamic State and from the so-called 'Cyber Caliphate'. In response, the French government activated a cyber crisis cell for the first time ('Cyberattaques', 2015). These attacks, as well as earlier incursions, have been a leading rationale for the establishment and enhancement of French military cyberdefence capabilities (Hathaway et al., 2016, p. 10).

The French military cyberdefence model implies a strict division between defensive and offensive capabilities with the aim of facilitating the acceptance of state intervention in the security of information systems, hoping that providers will be more willing to cooperate if they can be sure that their information is not used for conducting offensive missions (SGDSN, 2018, p. 5). ANSSI is responsible for most protective capabilities, with the protection of military networks delegated to the commander of cyberdefence. The Ministry of the Armed Forces (MAF) can employ active cyberwarfare and offensive operations under the authority of the President.[6] French military efforts in cyberspace have drastically transformed in recent years, especially in comparison to 2009, when the Conficker virus compromised unclassified French military intranets which grounded some fighter planes of the French Navy (Willsher, 2009). Its military cyberdefence policies are laid out in the Cyber Defence Pact of 2014 (Ministry of Defence, 2014) and more recently in 2019, when the French Minister of the Armed Forces

[6] The French Ministry of Defence was renamed to Ministry of the Armed Forces in 2017. Both iterations are used in their respective time periods.

unveiled a defensive policy and an offensive doctrine for military cyberdefence (Ministry of the Armed Forces, 2019a, 2019b).

On the basis of the 2013 White Paper, the Cyber Defence Pact listed 50 measures to improve the organisation of cyberdefence, including by strengthening operational command, furthering the network of a cyber reserve force, and the creation of a Centre of Excellence for Cyberdefence in Brittany (Ministry of Defence, 2014, p. 5). It vowed to make cyberdefence an aspect at every level of exercises conducted by the armed forces (p. 9). The pact was introduced alongside a €1 billion investment package to reach its goals. In 2017, operational and coordinating responsibilities for MAF cyberdefence transferred from the Operation General Cyber to the newly created Cyber Command (COMCYBER). It is tasked with defending the armed forces networks and the preparation of offensive capabilities under the authority of the President (Ministry of the Armed Forces, 2019a, p. 5). COMCYBER directs the operations of the Analysis Centre for Defensive Cyber Operations (CALID), which is responsible for continually monitoring threats to military networks and for directing defensive responses (Baezner, 2018, p. 16). To this end, it also houses MilCERT, the MAF CERT-team. Moreover, COMCYBER works closely with the procurement directorate DGA MI to develop cybercapabilities in the armed forces (Ministry of the Armed Forces, 2019a, p. 11).

In regard to defensive capabilities, the MAF recognises the need to make all users of its digital networks aware of the accompanied risks. Therefore, it has established security operating centres (SOC) in all layers of the organisation, including all branches of the military (Ministry of the Armed Forces, 2019a, p. 8). These SOCs are regarded as the first line of defence in detecting cyberattacks, with CALID overseeing their operations under the responsibility of COMCYBER. Besides enhancing a culture of cybersecurity in its own operations, the doctrine aims to do the same with third parties related to the MAF, including its industrial suppliers. It will propose a convention that clarifies the different roles and responsibilities of its suppliers (Ibid.) Observing that cybersecurity efforts can be undermined through a single fallible point, the ministry attempts to take an coherent and integrated approach across different layers.

Before the publication of the offensive doctrine, the armed forces were focused mainly on network defence with an element of active defence, while the intelligence services were responsible for more sensitive, offensive operations (Laudrain, 2019). Under the new doctrine, the MAF became responsible for offensive operations in cyberspace. These are classified into three categories: evaluating adversarial capacities; reducing or neutralising enemy capacity; and modifying perceptions of the enemy by discreet alteration of their data (Ministry of the

Armed Forces, 2019a, p. 6). COMCYBER is responsible for the planning and coordination of offensive operations and for the involvement of intelligence services or allies. France has signed the NATO Cyber Defence Pledge, encouraging other member states to develop their cybercapabilities (p. 10). Finally, France pledges to fulfil a 'motor function' in creating a shared military cybersecurity culture on the European level, with the ambition to realise interoperational capabilities with its European partners.

In the Military Programming Law of 2019-2025, the government aims to raise the number of 'cyber combatants' from 3,000 to 4,000 with an additional investment of €1.6 bln (Ministry of the Armed Forces, 2018a, p. 4). Moreover, its citizen cyber reserve consists of 4,400 reservists, spread out over 50 different permanent posts (Ministry of the Armed Forces, 2018b). Together with the earlier investments through the Cyber Defence Pact, France has heavily invested in shaping its military cyberdefence capabilities while integrating a cybersecurity culture in all layers of the organisation. These investments point to a better understanding of how to achieve redundancy in governance logics. With a structured line of command, clarified responsibilities for third parties and a public offensive doctrine based on international legal norms, France is on its way to becoming a considerable power in military cyberdefence.

Countering cybercrime through education and raising awareness

One of the priorities of the French National Digital Security Strategy is to enhance efforts against cybercrime and to assist victims of cybermalevolent acts (Valls, 2015, p. 21). Since the late 1990s, the Gendarmerie, the French military police force, has established several units that are responsible for countering cybercrime in France. In 2016, the Ministry of the Interior (MoI), responsible for the police and the Gendarmerie, set out its three cybersecurity policy pillars, which are to proactively tackle cybercrime; to establish a dialogue with private partners; and to adapt international and national legal frameworks (Ministry of the Interior, 2016). Besides these wide-ranging objectives, the ministry publishes an annual report detailing both cyberthreats and the response taken by the Gendarmerie (Ministry of the Interior, 2019).

France has ratified the Budapest Convention in 2006 and, as discussed above, is making efforts to universalise the norms agreed upon in the convention and to advocate for an increased legal cooperation on cybercrime within the EU. Domestically, cybercrime is incorporated into the Penal Code by the Godfrain Law, with the Budapest Convention implemented in the LOPPSI 1 and 2 acts (Häger & Dackö, 2017, p. 8). When the latter was introduced in 2010, it elicited controversy over its regulation of the internet with *Der Spiegel* stating that it would

make France the strictest country in Europe when it came to internet regulation and surveillance (Simons, 2010).

Organisationally, the MoI has appointed a 'cyber prefect' responsible for coordinating initiatives related to cybercrime and for implementing the action plan of the ministry (Hathaway et al., 2016, p. 11). Responsible for the most complex cases are the cyberexperts of the national criminal research institute of the Gendarmerie (IRCGN), who cooperate with Interpol and Europol on cross-border cases (Gendarmerie, n.d.). On the local level, the Gendarmerie employs P-NTECH officers in each brigade who are trained to do take-in of cybercrime reports and who carry out seizure operations of digital evidence (Ministry of the Interior, 2019, p. 12). As of 2018, each gendarme student will receive this training during their education. 4,300 C-NTECH officers have been trained to deal with simple analyses of phone and computer data, who can follow additional training to carry out more complex researches. Finally, 250 NTECH officers trained at the University of Technology in Troyes are responsible for technical investigations in more complex cases related to criminal groups and the digital forensic side (p. 13).

Public-private partnerships are regarded as an important aspect of the strategy to counter cybercrime, especially through information-sharing and by cooperating with online platforms (Ministry of the Interior, 2019, p. 116). The Permanent Contact Group (GCP) was established after the terrorist attack of 2015, consisting of officials from the MoI together with representatives from major corporations such as Apple, Google, Microsoft and Facebook. It was set up with the goal of improving the reporting and removal of illegal content and to facilitate data requests from French criminal investigators. PPPs are also established to raise awareness among French enterprises and the population at large, notably for the education of pupils at lower and higher education. An example is the publication of the "Les As du Web" comic book in cooperation with the Information Systems Security Association, meant to teach cybersecurity best practices to children aged 7 to 11 (p. 104).

In all, the MoI has adapted to an emerging threat of cyberattacks by adopting new basic assumptions and institutes, with basic training on how to deal with such attacks incorporated into the education of each new officer. Through public-private partnerships and awareness campaigns, the MoI has attempted to diffuse its norms in cyberspace and to create a culture of cybersecurity on all levels. However, despite these efforts some challenges in countering cybercrime remain. Reporting of cybercrime to the authorities still remains low, hampering targeted prevention efforts (Ministry of the Interior, 2019, p. 129). Moreover, the MoI has identified a lack of coherence in cybercrime prevention approaches on the regional level (p. 130).

Cybersecurity in France: central direction and local integration

From the creation of the national Minitel service in the early 1980s and after its demise due to the introduction of the Internet, France has become a well-connected country with a clear ambition to become a world player on cybersecurity-related issues such as international legal norms and military cyberdefence. After a review of national defence and security policy in 2008, cyberattacks were classified as a major threat, in turn spurning the development of a national cybersecurity ecosystem. Although France took a centralised approach with sparse attention to cooperation with the private sector in its initial strategies, it has moved towards a more flexible ecosystem through including diverse stakeholders and efforts to create convergence on common national and international norms and standards in cyberspace.

France has stooled its cybersecurity logic on the protection of sovereign interests, including its ability to make decisions in times of crisis. For the French government, digital autonomy remains an objective, both on the national as well as the European level. Through the explication and diffusion of norms such as an open cyberspace and the application of international law, together with capability-building efforts with EU and NATO partners, France aims to become a world power in cyberdefence. It has matched this ambition with substantial investments in capability-building and recruitment of personnel, also aimed at consolidating a national industrial cybersecurity base, indicating a move from efficiency to redundancy logics.

French approaches to consolidating this base, as well as to setting industry standards, have been conducted through centralised direction and guidance such as identifying important security firms needed for digital autonomy and providing regulatory powers to ANSSI in the field of vital infrastructure. Although this approach might seem indicative of a type-1 system where the state controls resource and information allocation, the French programme is dependent on cooperation with the private sector and leaves room for shared governance through information-sharing platforms. The French cybersecurity ecosystem, like the Dutch, is moving towards a type-3 ‘Openness and Adaptability’ approach, owing to its consolidation of institutional structures such as ANSSI or COMCYBER and to its attempt to create an understanding of cybersecurity at all levels of government, be that in different ministries, army branches or police units.

Conclusion

Resilience has gained ground as a widely shared objective for increasing security in cyberspace. Despite its omnipresence, interpretations of resilience in cyberspace, and in security studies in general, differ from state to state and author to author. There is an inherent conceptual unclarity. Through employing and expanding on the framework of Christou (2016) for categorising different conceptualisations of resilience as security in cyberspace, this thesis has discussed what conditions are foundational for creating a national cybersecurity ecosystem that can be said to be resilient. In addition, through explicating the pathways that the Netherlands and France have taken to doing so, the research sheds light not only on what these systems are, but also on how they came to be. Doing so has the potential to be an explanatory device for researching the approaches other countries have taken towards achieving resilience as security in cyberspace.

The research question this thesis has focused on is *To what extent have France and the Netherlands achieved resilience in their cybersecurity approaches, as defined by Christou (2016)?*. It is divided into the sub-questions *As what type of resilience can the Dutch and French approaches be characterised?* and *What are the pathways that have led to their respective approaches to cybersecurity?* Given the relatively similar, advanced states of both countries' cybersecurity policies and their vastly different institutional and bureaucratic cultures, the hypothesis *H: France and the Netherlands have achieved openness and adaptability in their approach to cybersecurity, but have developed different pathways towards this outcome* was formulated. Owing to these questions, especially the question concerning the pathways towards approaches to cybersecurity, the model put forward by Christou (2016) requires additional empirical underpinning and the formulation of indicators for achieving the modelled conditions.

Although resilience has a multitude of interpretations in the security studies literature, a common denominator in security as resilience approaches is the idea of networked partnerships, where policies and strategies drafted on the national level decentralise responsibility to local networks of authority and non-governmental actors. In line with this conceptualisation, Christou identifies three distinct approaches to cybersecurity governance based on the typology of resilience by Handmer and Dovers (1996). Type 1 approaches, or 'Resistance and Maintenance', are characterised by hierarchical governance and state control over resource allocation and information. Such approaches aim to maintain the status quo by resisting change, while projecting outward stability. While this approach is defined by its rigidity, type 2 'Change at Margins' approaches draw from linear risk assessment models. They are characterised by a

problem-solving approach that disfavours systemic change. Finally, the type-3 model, 'Openness and Adaptability', is mentioned as the preferred approach in creating an effective security as resilience cybersecurity ecosystem due to its emphasis on flexibility. The third approach is marked by its capacity to adapt to external shocks based on an ecosystem designed around the concept of redundancy over efficiency. The latter can be said to be the most effective in achieving resilience as security due to the inherent complexity of the cybersecurity threat landscape and the diffusion of resources and information between public and private actors.

Six conditions are put forward that outline the presence of a type-3 approach to achieving resilience as cybersecurity in cyberspace. In this research, these conditions were not used as benchmarks or norms but rather as indicators of a prevalent resilience type, given that this thesis did not concern itself with the supposed effectiveness of such a system but rather with the nature of the system itself. Through the comparison of the cybersecurity approaches of the Netherlands and France, two positive cases likely to have achieved effective resilience, the applicability of the model and its different possible outcomes are tested. In both cases, the conditions formulated by Christou have proven to cover defining characteristics of both Dutch and French cybersecurity approaches, such as the necessity for cooperation between public and private parties and the governments' attempts to foster a culture of cybersecurity in all levels and among stakeholders including institutions, private entities, individual citizens and the international community at large. By tracing the pathways the Netherlands and France have taken to arrive at their current approach, it emerged that both countries started from largely different premises, only to converge in their approach in recent years.

In its first national strategies for developing a cybersecurity ecosystem, the Dutch approach took a middle path between type-2 and type-3 methods, whereas the French approach initially took a more type-1 approach only to move towards a type-3 conceptualisation in its later strategies. From the start, however, both countries were found to adhere to different conditions of the Christou model, with divergence on one or two conditions explaining their categorisation as mixed-model approaches. After discussing the different or comparable results per condition, the conclusion continues with analysing the divergent logics of cybersecurity and notes on the model itself.

Both the Netherlands and France have demonstrated a preparedness to adopt new operating assumptions and, most prominently, institutional structures. These are the CSR and NCSC in the Netherlands and ANSSI in France as nodal actors in a networked system of public and private parties and the DCC and COMCYBER as new command structures in military cyberdefence. New operating assumptions, including the participation of the private sector in

the creation of regulations and in sharing information, drive these institutional structures, most notably in the CSR in the Netherlands. This advisory body linked to the cabinet consists of representatives from both public, private and academic parties. However, the cases differ in the extent to which these new structures and operating assumptions are matched with funding that could leave space for redundancy in order to support complexity in governance logics. Whereas the French government made firm investments in ANSSI, military cyberdefence and the wider cybersecurity industry, the Netherlands appeared to be somewhat hesitant in doing so at first. Only the third strategy was matched with additional funding that has still left some questioning its sufficiency.

Given the predominance of private actors in cyberspace, the case study found that both countries emphasise the importance of public-private cooperation and partnerships in achieving their cybersecurity strategies, albeit to a dissimilar degree. The Netherlands, with its *polder* model approach to governance, involved protracted involvement of private parties in the setting of regulations and the formulation of national strategies, indeed recognising public-private co-operation as the basis for their approach. This large amount of actors with diffuse responsibilities could, however, have the potential to stagger decision-making in times of crisis. France, with its more centralised approach to governance, has been somewhat reluctant to realise its strategies through localised public-private networks. Although it does recognise the value of cooperation with the private sector and involves private actors in fields ranging from education to combating crime, most emphasis in its strategies is on maintaining an industrial strategic autonomy and on government regulation over coordinated self-regulation.

France is a major actor in attempting to create convergence amongst stakeholders on international norms in cyberspace, through sharing its doctrine for offensive operations and by campaigning for the development of a shared European military cybersecurity culture and operational capabilities. It has been argued that in doing so, France pursues a global leadership role in cyberdefence by projecting its power. Internationally, the Netherlands has a narrower scope in advancing military legal standards, but emphasises the evolution of internet freedom norms through co-founding the Freedom Online Coalition. Both countries have taken considerable steps in promoting and developing cybersecurity standards for and with private actors on the domestic level.

Movements towards the evolution of a culture of cybersecurity on all levels and among all stakeholders can be witnessed in both cases. France and the Netherlands include cybersecurity-related aspects in military mission planning and aim to facilitate a basic understanding of cybercrime in their respective police units. Despite still having a substantial way to go in the

latter, both countries have prioritised doing so. In fostering awareness and promoting education on cybersecurity, France has undertaken large-scale programmes catered especially to young students and the Dutch government has launched several national campaigns on responsible use of the internet. Notably, the French and Dutch governments have involved private actors in these awareness campaigns as well as in promoting scientific research and academic education. With the sum of endeavours and strategies, both countries have made strident developments from their first strategies and reviews to arrive at a more coherent and integrated approach to achieving security as resilience in cyberspace.

The most poignant difference between both states is found in the logics underpinning their cybersecurity strategies. Although both the Netherlands and France employ a dual logic of enhancing security against new threats while promoting national economic and industrial growth, they do so with differing rationalisations. For France, increasing security is directly linked to the preservation of national sovereignty and fundamental interests, with industrial maturity serving the same purpose. On the other hand, the Dutch strategy recognised achieving security in cyberspace as cornerstone for ensuring its function as a 'Digital Gateway to Europe' and related economic prerogatives. In other words, where the Dutch government emphasises a secure cyberspace as a condition for economic growth, the French government regards industrial growth as a condition for achieving national security.

Recommendations for future research

The Dutch and French approaches to cybersecurity are embedded in a wider European context. Their strategies are driven by European values such as the freedom of expression and internet freedom. Moreover, in line with the EU strategy, both countries recognise that sharing responsibility for achieving resilience as security in cyberspace is an essential component in doing so. Seeing as how both Dutch and French strategies have more or less converged towards an 'Openness and Adaptability' model raises the question of how this has happened. Could this be attributed to a better understanding of what it takes to achieve effective resilience as security or could it rather be due to a normative convergence of effective resilience on the European level? Future research on the norm-setting role of the European Union and its member states in cybersecurity has the potential to contribute to the understanding of the influence European countries and the EU have on each other in the formulation of cybersecurity strategies by member states.

In addition, given that France and the Netherlands were selected as positive cases based on their relatively high ranking on cybersecurity-related metrics, this research has

predominantly shed light on what pathways and conditions underpin the cybersecurity ecosystems of states that can be considered to have an effective approach. It is not unlikely to contemplate that other European states have taken a similar approach in their national strategies, only to find themselves on the lower end of such cybersecurity metrics. If states adhere to similar principles in their policy-setting, but do not achieve similar outcomes, it raises the question of how this divergence can be explained and what implications can be drawn for the state of the EU-wide cybersecurity ecosystem.

Resilience in cybersecurity is widely-discussed subject in security studies, this research has contributed to this debate by demonstrating how to conceptualise and analyse conditions that can be said to lead to a resilient cybersecurity ecosystem. By benchmarking and tracing policy narratives, the use of the Christou model covers a broad set of factors such as coherence, public-private partnerships and assumptions of redundancy, which, in the academic literature on resilience, are regarded as crucial factors in fostering a resilient approach to cyberspace. With the Netherlands and France taken as cases for this thesis, future research on the applicability of this model to other European countries and the EU itself has the potential to shed light on the state of resilience and progress towards creating it in the European cybersecurity ecosystem.

Bibliography

Alert Online. (2020, April 29). *Over Alert Online* (https://www.alertonline.nl/) [Text/html]. Alert Online; Alert Online. https://www.alertonline.nl/over-deze-campagne

AMS-IX. (2019). *AMS-IX Amsterdam*. AMS-IX. https://www.ams-ix.net/ams

ANSSI. (2011). *Information systems defence and security: France's strategy*. Agence Nationale de la Sécurité des Systèmes d'Information.

Baezner, M. (2018). *National Cybersecurity and Cyberdefense Policy Snapshots: France*. Centre for Security Studies.

Baldwin, D. A. (1997). The concept of security. *Review of International Studies*, *23*, 5–26.

Baumard, P. (2017). *Cybersecurity in France*. Springer International Publishing. https://doi.org/10.1007/978-3-319-54308-6

Bendiek, A., Bossong, R., & Schulze, M. (2017). *The EU's Revised Cybersecurity Strategy. Half-Hearted Progress on Far-Reaching Challenges* (SWP Comments 47, pp. 1–7). German Institute for International and Security Affairs.

Betz, D. J., & Stevens, T. (2011). Power and cyberspace. *Adelphi Series*, *51*(424), 35–54. https://doi.org/10.1080/19445571.2011.636954

Blatter, J., & Haverland, M. (2012a). Causal-Process Tracing. In *Designing Case Studies: Explanatory Approaches in Small-N Research* (pp. 79–143). Palgrave Macmillan. http://ebookcentral.proquest.com/lib/leidenuniv/detail.action?docID=931717

Blatter, J., & Haverland, M. (2012b, September). *Two or three approaches to explanatory case study research?* Annual Meeting of the American Political Science Association, New Orleans.

Boeke, S. (2016). *First Responder or Last Resort? The role of the Ministry of Defence in national cyber crisis management in four European Countries*. https://openaccess.leidenuniv.nl/handle/1887/46615

Boeke, S. (2018). Hackers, wiz kids, en offensieve cyberoperaties: Uitdagingen voor het Defensie Cyber Commando. *Atlantisch Perspectief*, *5*(42), 27–30.
Boekhoorn, P. (2019). *De aanpak van cybercrime door regionale eenheden van de politie—Van intake van cybercrime naar opsporing en vervolging*. BBSO.
Bossong, R., & Wagner, B. (2017). A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime, Law and Social Change*, *67*(3), 265–288. https://doi.org/10.1007/s10611-016-9653-3
Bot, W., & Hengstz, K. (2019). *Nationaal Cybersecurity Bewustzijnsonderzoek 2019: Cyberbewustzijn en vaardigheden onder de Nederlandse (beroeps)bevolking* (p. 60). Motivaction International B.V.
Broeders, D. (2014). *Investigating the Place and Role of the Armed Forces in Dutch Cyber Security Governance*. Netherlands Defence Academy. http://rgdoi.net/10.13140/RG.2.1.3974.3849
Cabinet Office. (2011). *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world* (p. 43).
Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43–62. https://doi.org/10.1111/1468-2346.12504
Carrapico, H., & Barrinha, A. (2017). The EU as a Coherent (Cyber)Security Actor? *JCMS: Journal of Common Market Studies*, *55*(6), 1254–1272. https://doi.org/10.1111/jcms.12575
Carrapico, H., & Barrinha, A. (2018). European Union cyber security as an emerging research and policy field. *European Politics and Society*, *19*(3), 299–303. https://doi.org/10.1080/23745118.2018.1430712
CBS. (2018). *Cybersecuritymonitor 2018: Een verkenning van dreigingen, incidenten en maatregelen*. Centraal Bureau voor de Statistiek.
CBS. (2019). *Nederland langs de Europese meetlat 2019*. Centraal Bureau voor de Statistiek. https://www.cbs.nl/nl-nl/publicatie/2019/20/nederland-langs-de-europese-meetlat-2019
Christou, G. (2016). *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. Palgrave Macmillan.
Clark, K., Stikvoort, D., Stofbergen, E., & van den Heuvel, E. (2014). A Dutch Approach to Cybersecurity through Participation. *IEEE Security & Privacy*, *12*(5), 27–34. https://doi.org/10.1109/MSP.2014.83
CNIL. (n.d.). *Le collectif Educnum | EDUCNUM*. Retrieved 25 June 2020, from https://www.educnum.fr/fr/le-collectif-educnum
Coaffee, J., & Fussey, P. (2015). Constructing resilience through security and surveillance: The politics, practices and tensions of security-driven resilience. *Security Dialogue*, *46*(1), 86–105. https://doi.org/10.1177/0967010614557884
CSR. (2020, February 27). *Cyber Security Council* [Webpagina]. Ministerie van Justitie en Veiligheid. https://www.cybersecurityraad.nl/index-english.aspx
CTIVD. (2019). *Voortgangsrapportage III: De werking van de Wiv 2017* (No. 66). Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten.
Cyberattaques: L'armée a activé pour la première fois une cellule de crise. (2015, January 17). *Le Monde.fr*. https://www.lemonde.fr/pixels/article/2015/01/17/cyberattaques-l-armee-a-active-pour-la-premiere-fois-une-cellule-de-crise_4558160_4408996.html
De Bruijne, M., Boin, A., & Van Eeten, M. (2010). Resilience: Exploring the Concept and Its Meanings. In C. C. Demchak, A. Boin, & L. K. Comfort (Eds.), *Designing Resilience: Preparing for Extreme Events*. University of Pittsburgh Press.
de Crespigny, M. (2012). Building cyber-resilience to tackle threats. *Network Security*, *2012*(4), 5–8. https://doi.org/10.1016/S1353-4858(12)70024-7
Delerue, F., Desforges, A., & Géry, A. (2019, April 23). A Close Look at France's New Military Cyber Strategy. *War on the Rocks*. https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/
Delerue, F., & Géry, A. (2018, March 23). France's Cyberdefense Strategic Review and International Law. *Lawfare*. https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law
D'Elia, D. (2018). Industrial policy: The holy grail of French cybersecurity strategy? *Journal of Cyber Policy*, *3*(3), 385–406. https://doi.org/10.1080/23738871.2018.1553988

Demchak, C. (2012). Cybered Conflict, Cyber Power, and Security Resilience as Strategy. In D. S. Reveron (Ed.), *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (pp. 121–136). Georgetown University Press.

Digital Trust Center. (n.d.). *Over het Digital Trust Center | Digital Trust Center*. Digital Trust Center. Retrieved 27 May 2020, from https://www.digitaltrustcenter.nl/over-het-digital-trust-center

DomainTools. (2019). *Domain Count Statistics for TLDs*. DomainTools. http://research.domaintools.com/statistics/tld-counts/

Dunn Cavelty, M. (2013). A Resilient Europe for an Open, Safe and Secure Cyberspace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2368223

Dunn Cavelty, M. (2018). Europe's cyber-power. *European Politics and Society*, *19*(3), 304–320. https://doi.org/10.1080/23745118.2018.1430718

Dunn Cavelty, M., & Prior, T. (2013). *Resilience in security policy: Present and future* (No. 142; CSS Analysis in Security Policy). Center for Security Studies. http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analysis-142-EN.pdf

Dunn-Cavelty, M., & Suter, M. (2009). Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, *2*(4), 179–187. https://doi.org/10.1016/j.ijcip.2009.08.006

E Silva, K. (2013). Europe's fragmented approach towards cyber security. *Internet Policy Review*, *2*(4), 1–8. https://doi.org/10.14763/2013.4.202

ENISA. (2011). *Inter-X: Resilience of the Internet Interconnection Ecosystem*. ENISA.

ENISA. (2012). *National Cyber Security Strategies: Practical Guide on Development and Execution*. ENISA. https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide

ENISA. (2018). *Cyber Europe 2018: After Action Report*. ENISA.

European Commision. (2017). *Digital Transformation Monitor: France: Industrie du futur*. European Commision. https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Industrie%20du%20Futur%20v1.pdf

European Commission. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. European Commission.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, 32013L0040, EP, CONSIL, OJ L 218 (2013). http://data.europa.eu/eli/dir/2013/40/oj/eng

European Commission. (2020a). *Digital Economy and Society Index (DESI) 2020: France*. European Commission.

European Commission. (2020b). *Digital Economy and Society Index (DESI) 2020: Thematic chapters*. European Commission.

Folke, C. (2006). Resilience: The emergence of a perspective for social–ecological systems analyses. *Global Environmental Change*, *16*(3), 253–267. https://doi.org/10.1016/j.gloenvcha.2006.04.002

Gendarmerie. (n.d.). *Département Informatique-Electronique (INL)*. Gendarmerie. Retrieved 27 June 2020, from /pjgn/IRCGN/Division-Criminalistique-Ingenierie-et-Numerique-DCIN/Departement-Informatique-Electronique-INL

Government of Romania. (2013). *Cyber security strategy of Romania*. Government of Romania.

Governo de Portugal. (2015). *National Cyberspace Security Strategy Portugal*. Governo de Portugal.

Hadji-Janev, M. (2014). Toward Effective Naitonal Cyber Security Strategy: The Path Forward for Macedonia. In E. Braman, P. Susmann, & A. Vaseashta (Eds.), *Cyber Security and Resiliency Policy Framework* (pp. 57–64). IOS Press.

Häger, E. W., & Dackö, C. (2017). *Cybersecurity Law Overview: A Report by Mannheimer Swartling*. Mannheimer Swartling.

Handmer, J. W., & Dovers, S. R. (1996). A Typology of Resilience: Rethinking Institutions for Sustainable Development. *Industrial & Environmental Crisis Quarterly*, *9*(4), 482–511. https://doi.org/10.1177/108602669600900403

Hathaway, M., Demchak, C., Kerben, J., McArdle, J., & Spidalieri, F. (2016). *France: Cyber Readiness at a Glance* (Cyber Readiness Index 2.0, p. 32). Potomac Institute for Policy Studies.

Hathaway, M., & Spidalieri, F. (2017). *The Netherlands: Cyber Readiness at a Glance* (Cyber Readiness Index 2.0). Potomac Institute for Policy Studies.
Herrington, L., & Aldrich, R. (2013). The Future of Cyber-Resilience in an Age of Global Complexity. *Politics*, *33*(4), 299–310. https://doi.org/10.1111/1467-9256.12035
Hollande, F. (2013). *French White Paper Defence and National Security 2013*.
Holling, C. S. (1996). Engineering Resilience versus Ecological Resilience. In P. C. Schulze (Ed.), *Engineering Within Ecological Constraints* (pp. 31–44). National Academy Press. https://www.nap.edu/read/4919/chapter/4#32
Hustinx. (2013). *Opinion of the European Data Protection Supervisor on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a 'Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union*. European Data Protection Supervisor. https://edps.europa.eu/sites/edp/files/publication/13-06-14_cyber_security_en.pdf
ITU. (2008). *ITU-T X.1205 Overview of cybersecurity*. ITU. https://www.itu.int/rec/T-REC-X.1205-200804-I
ITU. (2017). *Global Cybersecurity Index 2017* (p. 78). International Telecommunications Union.
Joseph, J. (2013). Resilience in UK and French Security Strategy: An Anglo-Saxon Bias? *Politics*, *33*(4), 253–264. https://doi.org/10.1111/1467-9256.12010
Juncker, J.-C. (2017, September 13). *EU State of the Union Address 2017*. European Commission Press Release Database. http://europa.eu/rapid/press-release_SPEECH-17-3165_en.htm
Motie van het lid Knops c.s., 32 123 X, Tweede Kamer der Staten-Generaal, 2009–2010, 2009–2010 66 (2009).
Laudrain, A. P. B. (2019, February 26). France's New Offensive Cyber Doctrine. *Lawfare*. https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine
Longstaff, P. H. (2005). *Security, Resilience, and Communication in Unpredictable Environments Such as Terrorism, Natural Disasters, and Complex Technology*. Harvard University Center for Information Policy Research.
Luthar, S. S. (2003). *Resilience and Vulnerability: Adaptation in the Context of Childhood Adversities*. Cambridge University Press.
Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018). Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls. *Sensors (Basel, Switzerland)*, *19*(1). https://doi.org/10.3390/s19010019
Ministry of Defence. (2012). *The Defence Cyber Strategy*. Ministry of Defence of the Kingdom of the Netherlands.
Ministry of Defence. (2013). *Finland's Cyber security Strategy*. Secretariat of the Security and Defence Committee.
Ministry of Defence. (2014). *Pacte Défense Cyber: 50 mesures pour changer d'échelle*. Ministère de la Défense.
Ministry of Defence. (2018a). *Defence White Paper 2018: Investing in our people, capabilities and visibility*. Ministry of Defence of the Kingdom of the Netherlands.
Ministry of Defence. (2018b). *Defensie Cyber Strategie 2018: Investeren in digitale slagkracht voor Nederland*. Ministry of Defence of the Kingdom of the Netherlands.
Kamerbrief Integrale aanpak cybercrime, (2018) (testimony of Ministry of Justice and Security).
Ministry of Security and Justice. (2011). *The National Cyber Security Strategy (NCSS): Strength through cooperation*. Ministry of Security and Justice. https://english.nctv.nl/binaries/cyber-security-strategy-uk_tcm32-83648.pdf
Ministry of Security and Justice. (2012, September 4). *Joint Cyber Security exercise with Germany—News item—Government.nl* [Nieuwsbericht]. Ministerie van Algemene Zaken. https://www.government.nl/latest/news/2012/09/04/joint-cyber-security-exercise-with-germany
Ministry of Security and Justice. (2014). *National Cyber Security Strategy 2: From awareness to capability*. Ministry of Justice and Security of the Kingdom of the Netherlands.

Ministry of Security and Justice. (2018). *National Cyber Security Agenda: A cyber secure Netherlands*. Ministry of Justice and Security of the Kingdom of the Netherlands.
Ministry of the Armed Forces. (2018a). *Projet de loi de programmation militaire 2019-2025: Synthèse: Un LPM de renouveau*. Ministère des Armées.
Ministry of the Armed Forces. (2018b, October 17). *La cyberdéfense*. Ministère des Armées. https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/la-reserve-de-cyberdefense
Ministry of the Armed Forces. (2019a). *Eléments publics de doctrine militaire de lutte informatique offensive*. Ministère des Armées.
Ministry of the Armed Forces. (2019b). *Politique ministérielle de lutte informatique défensive*. Ministère des Armées.
Ministry of the Interior. (2016, January 28). *Cybersecurity: The Government's strategy*. Gouvernement.Fr. https://www.gouvernement.fr/en/cybersecurity-the-government-s-strategy
Ministry of the Interior. (2019). *État de la menace liée au numérique en 2019: La réponse du Ministère de l'Intérieur*. Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces.
Pelk, H. (2017, April 3). *Henk Ras over het Defensie Cyber Commando en de digitale veiligheid (deel 2)*. ITNEXT. https://itnext.io/henk-ras-over-het-defensie-cyber-commando-en-de-digitale-veiligheid-deel-2-5a9847a9dca8
Philippe, É. (2017). *Le grand plan d'investissement 2018-2022: Dossier de presse*. Office of the Prime Minister. https://www.gouvernement.fr/sites/default/files/document/document/2017/09/dossier_de_presse_-_le_grand_plan_dinvestissement_2018-2022.pdf
Politie.nl. (2018, April 25). *Politie sluit grootste DDoS-website in Operation Power Off*. Politie.nl. https://www.politie.nl/nieuws/2018/april/25/politie-sluit-grootste-ddos-website-in-operation-power-off.html
Rademaker, M., Faesen, L., Van Lieshout, K., & Abdalla, M. (2016). *Dutch Investments in ICT and Cybersecurity: Putting it in perspective*. The Hague Centre for Strategic Studies.
Regards Citoyen. (2018, April 18). *Commission des finances, du contrôle budgétaire ed des comptes économiques de la nation: Réunion du 18 avril 2018 à 14h35*. Nos Sénateurs. https://www.nossenateurs.fr/seance/17644#inter_743bb480874fd68a748735069807262b
Robinson, N. (2014). *EU cyber-defence: A work in progress*. European Union Institute for Security Studies.
Sachwald, F. (1997). *Colbertism in ICT: Lessons from the French experience* (p. 32). l'Institut français des relations internationals.
Sarkozy, N. (2008). *The French White Paper on Defence and National Security*. Présidence de la République.
SGDSN. (2018). *Strategic Review of Cyber Defence*. Secrétariat général de la défense et de la sécurité nationale. http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf
Simons, S. (2010, February 17). The Big Brother of Europe? France Moves Closer to Unprecedented Internet Regulation. *Der Spiegel International*. https://www.spiegel.de/international/europe/the-big-brother-of-europe-france-moves-closer-to-unprecedented-internet-regulation-a-678508.html
Sliwinski, K. F. (2014). Moving beyond the European Union's Weakness as a Cyber-Security Agent. *Contemporary Security Policy*, *35*(3), 468–486. https://doi.org/10.1080/13523260.2014.959261
Smeets, M. (2018). Cyber: 'People, people, people': Vragen over het DDC en het inzetten van cyberactiviteiten. *Atlantisch Perspectief*, *6*(42), 30–34.
Sterbenz, J. P. G., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, *54*(8), 1245–1265. https://doi.org/10.1016/j.comnet.2010.03.005
Toucas, B. (2018, March 29). With Its New 'White Book,' France Looks to Become a World-Class Player in Cyber Space. *War on the Rocks*. https://warontherocks.com/2018/03/with-its-new-white-book-france-looks-to-become-a-world-class-player-in-cyber-space/

Tran, H., Campos-Nanez, E., Fomin, P., & Wasek, J. (2016). Cyber resilience recovery model to combat zero-day malware attacks. *Computers & Security*, *61*, 19–31. https://doi.org/10.1016/j.cose.2016.05.001

Valls, M. (2015). *French National Digital Security Strategy*. Secrétariat général de la défense et de la sécurité nationale.

Van Bree, R., Nijeboer, R., Klerkx, G., Witteveen, L., & Monsma, E. (2016). *Cybercrime strategie 2020: Voor een veiliger Nederland, ook in het digitale domein*. Nationale Politie.

Van Lonkhuyzen, L., & Meeus, J. (2017, July 22). *Hoe tech-agenten de Onderwereld 2.0 te slim af waren*. NRC. https://www.nrc.nl/nieuws/2017/07/22/hoe-techno-agenten-de-onderwereld-20-te-slim-af-waren-12186839-a1567558

Van Lonkhuyzen, L., & Versteegh, K. (2018, December 18). Het cyberleger kan en mag nog weinig. *NRC*. https://www.nrc.nl/nieuws/2018/12/18/het-cyberleger-is-er-wel-maar-mag-weinig-a3099254

Verhagen, H. (2016). *De economische en maatschappelijke noodzaak van meer cyber security: Nederland digitaal droge voeten*. PostNL.

Walker, J., & Cooper, M. (2011). Genealogies of resilience: From systems ecology to the political economy of crisis adaptation. *Security Dialogue*, *42*(2), 143–160. https://doi.org/10.1177/0967010611399616

Wessel, R. A. (2015). Towards EU cybersecurity law: Regulating a new policy field. In N. Tsagourias & R. Buchan (Eds.), *Research Handbook on International Law and Cyberspace* (pp. 403–425). Edward Elgar Publishing. https://doi.org/10.4337/9781782547396

Wildavsky, A. (1988). *Searching for safety*. Transaction Books.

Willsher, K. (2009, February 7). French fighter planes grounded by computer virus. *Telegraph*. https://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html

Yin, R. K. (1998). The Abridged Version of Case Study Research: Design and Method. In L. Bickman & D. J. Rog (Eds.), *Handbook of Applied Social Research Methods* (pp. 229–260). Sage Publications.

Yin, R. K. (2003). *Case Study Research: Design and Methods* (Vol. 5). SAGE Publications.