Governance of cybersecurity communities

Understanding threat intelligence sharing as a collective action problem through incentivization of the National Detection Network

Xander Bouwman

student no. 4633180
research@xanderbouwman.com

Master thesis submitted to Delft University of Technology
in partial fulfilment of the requirements for the degree of

Master of Science
in Complex Systems Engineering and Management
Faculty of Technology, Policy and Management

To be defended in public on September 25 2018

Graduation chair	Prof.dr. M.J.G. van Eeten	Section Organization & Governance
First supervisor	Dr. M.E. Warnier	Section Multi-Actor Systems
External supervisor	Dr. K.P. Clark	National Cyber Security Centre
External supervisor	Ing. B. van der Kamp	National Cyber Security Centre

I extend my gratitude to those who shared their valuable time and ideas with me. This includes graduation committee members Michel van Eeten and Martijn Warnier, supervisors Kas Clark and Bob van der Kamp, colleagues at the National Cyber Security Centre of the Netherlands, and all experts and participants in the National Detection Network who agreed to be interviewed.

Digital document available at
xanderbouwman.com/research

Abstract

Organizations benefit from improved cybersecurity threat detection capabilities if they share information in a community of their peers. However, organizations are unlikely to share the sensitive information that is most valuable as this poses individual risks. Information sharing in cybersecurity communities therefore forms a collective action problem. Currently, cybersecurity information sharing is being studied primarily as a technological challenge. Drawing on theory from economics and the social sciences, this study proposes governance requirements to overcome individual interests and improve information sharing. These are used to design a governance structure for the case of the National Detection Network, a cybersecurity community initiated by the government of the Netherlands. The proposed governance meets interests of parties through a process of interactive decision-making in four phases, while incentivizing sharing of cybersecurity information. Lessons are drawn from the case for cybersecurity communities in general.

Contents

Chapter 1

Introduction

Businesses in the Port of Rotterdam were immobilized for weeks over the summer of 2017 due to the NotPetya malware. This caused considerable economic damage, as described by the National Coordinator for Security and Counterterrorism of the Netherlands (2018a). A growing number of such attacks in the digital domain is carried out.

In the same year, digital espionage resulted in the theft of valuable data from European companies in the fields of energy, high-tech, and chemical industry. Furthermore, 2017 saw an increase in attempts to gain access to vital infrastructures in Europe with the aim to sabotage them in a later stage. These two developments could have a significant impact on society, according to the General Intelligence and Security Service of the Netherlands (2018).

Traditional measures to protect against cybersecurity attacks, like firewalls or authorization schemes, aim to prevent unwanted access to a network. However, when defending against threat actors with advanced capabilities and abundant resources, traditional controls won't suffice. A digital arms race will eventually be lost if the opponent is sufficiently motivated.

1.1 Detection and threat intelligence sharing

Evidence from practice indicates that attackers often go undetected for an average of three months, if they are found at all (Mandiant 2018). During this time, attackers can engage in espionage or sabotage of systems, like infrastructure that provides drinking water to homes. Organizations that face targeted attacks must therefore work under the assumption that threat actors are already on their networks and add detection capabilities to their cybersecurity strategies in order to find them.

Measures for detection are readily available; passive and active automated monitoring systems exist that scan internal networks of organizations for properties of known attacks. Such properties include lists of IP-addresses spreading malware and hashes of malicious files. Knowing what to look for is therefore an essential part of successfully detecting threats.

These attack properties or *indicators* must be derived from experience with a certain threat in practice by having human analysts extract its properties to create reports or detection rules. The outcome of this process is referred to as 'threat intelligence'.

As peer organizations in for example the financial industry may face the same threats, sharing their cybersecurity threat intelligence allows them to detect or prevent attacks with which they have no prior experience while their peers do. Exchanging threat intelligence in a community of peers may therefore raise the overall security level of the community.

Peers can exchange their knowledge about threats over any medium, be it through face-to-face meetings or over the phone. Over the last years, a move toward automated

platforms for exchange of indicators and threat intelligence in a broad sense has developed (Sauerwein et al. 2017). Such platforms support collection, analysis, and sharing of information. While this technology supports information sharing and therefore is a step in the right direction, having the technology alone does not motivate organizations to share information.

1.2 Problem

There is a role for government in promoting information sharing in cybersecurity communities, as this benefits not only the organizations in the communities but all citizens relying on the services and infrastructures provided by them. In the case of vital infrastructures, such as telecommunications and the power grid, the willingness to share information and therefore the capability to detect cybersecurity threats is tied directly to national security.

However, decision-power of national governments is limited when it comes to many of the organizations that should most urgently engage in cybersecurity information sharing. The majority of vital infrastructures is in private hands, including energy companies, internet service providers, and financial institutions. In the case of the Netherlands, 80% of such critical infrastructures are private organizations (National Coordinator for Security and Counterterrorism of the Netherlands 2018b).

The government of the Netherlands has initiated the National Detection Network (NDN). One of the goals of this cybersecurity community is to support information sharing between public and vital sector organizations in the Netherlands (NCSC-NL 2018). Cooperation in this community has the potential to improve threat detection capabilities for Dutch public and vital sector organizations. Currently some 60 organizations are participating.

Positive network externalities will increase as more parties share information (Gordon, Loeb, and Lucyshyn 2003). However, information in the National Detection Network is currently primarily being shared by the system initiators. Based on community interviews conducted for this study, many participants in the community consume threat intelligence but do not share information back.

The research question of the thesis is: **How can information sharing in the National Detection Network be incentivized?**

Answering this question potentially improves information sharing in the National Detection Network, which benefits cybersecurity detection capabilities at Dutch public and vital sector organizations. These organizations deliver goods and services on which citizens of the Netherlands rely.

1.3 Approach

During a six-month internship at the National Cyber Security Centre (NCSC) of the Netherlands, the author studied the case of the National Detection Network through 18 interviews with stakeholders, participants, and experts. Recommendations were formulated for governance to improve information sharing in cybersecurity communities, drawing on a knowledge base of collective action theory. With these requirements, a process design was proposed for increasing information sharing in the National Detection Network.

The research question is operationalized using the following sub-questions.

1. What factors determine the level of information sharing in a cybersecurity community?

2. Are missing incentives limiting information sharing in the NDN?

3. What are requirements of governance that improves information sharing?

4. How can the NCSC shape governance in the NDN community?

1.4 Overview

The rest of this document is structured as follows. First, a knowledge base, method, and case study context are established for the study. Based on this, requirements to improve information sharing and a corresponding design for the National Detection Network community are proposed. Finally, the study's findings and designs are placed in context in order to draw conclusions.

Chapters in the document are structured along the lines of the sub-questions. An overview of the research flow is provided in the methodology chapter in Figure 3.2.

Chapter 2 considers the state of the art in cybersecurity information sharing technologies and practices in order to establish how and why individual organizations consume threat intelligence. A literature review of collective action theory aims to provide better understanding of the decision to engage in information sharing in cybersecurity communities.

Chapter 3 describes the methods used in the case study and interviews, as well as the methodology that is used to generate a design.

Chapter 4 establishes the case study of the National Detection Network, describing the history and current status of the community and its supporting technologies. Results of interviews with participants are presented in order to study the existence of a collective action problem in this community.

Drawing on the literature review and the description of interests in the National Detection Network, a design is proposed in two parts. Chapter 5 describes requirements community governance for improving information sharing.

Based on this, chapter 6 then proposes a governance structure with the aim to increase information sharing in the National Detection Network. The design describes an interactive decision-making process of four phases through which the community participants are incentivized to share information.

Chapter 7 discusses the findings of the case study and the proposed requirements and design. It considers if lessons on promoting information sharing in the National Detection Network can be generalized to cybersecurity communities in general.

Chapter 8 draws conclusions. It answers the main research question and places findings of the study into context.

Chapter 2

Threat intelligence and collective action

The literature review in this chapter lays the foundation for the rest of the study. The chapter answers the question: **What factors determine the level of information sharing in a cybersecurity community?**

Security of information technology is now a broad field, with attackers ranging from state-level actors to disgruntled employees, each with their own methods and goals to cause harm on an ICT network (National Coordinator for Security and Counterterrorism of the Netherlands 2018a).

Addressing a cybersecurity threat consists of five steps: to develop the organizational understanding necessary to manage risk, to develop safeguards, to detect the occurrence of a cybersecurity event, and to respond to and to recover from the event (NIST 2014).

This research focuses on detection of an attacker's presence on the network so that the defender may respond. The organizational capability to do this does not stand on its own. According to Fransen and Kerkdijk (2017), organizations develop resilience through four additive strategies:

1. Traditional prevention using simple controls;
2. Monitoring for attacks and limiting damage;
3. Anticipating attacks using threat intelligence; and
4. Automated response and recovery.

In order to be able to anticipate attacks in stage three, organizations need access to threat intelligence information. This consists of properties of attacker behaviour that can be used to take preventive steps and recognize an event when it occurs.

The first section of this chapter describes the practice of cybersecurity threat detection, which motivates the consumption of threat intelligence for organizations. It then considers the STIX taxonomy for describing threat intelligence.

Section 2.2 of this chapter goes into how cybersecurity communities have been sharing threat intelligence and how this is supported by digital platforms. An overview of these platforms is presented.

Section 2.3 describes the risks and benefits of participating in such communities. It discusses collective action problems, where individual rational behaviour leads to sub-optimal outcomes for a community.

In the final section of this chapter, a knowledge gap is identified in theory on cybersecurity information sharing. The first sub-question of the study is then answered.

2.1 Consumption of threat intelligence

According to the European body for cybersecurity ENISA (2018) a threat is *any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.* A threat could be malware or a phishing email, but also a power failure. Threats do not necessarily have to be motivated: also unintentional acts and natural disasters pose threats. Finding evidence of a threat is referred to as an event.

Cybersecurity threats are not markedly different from those in physical space. While there have arisen some new types of crime, like online banking fraud and ransomware extortion, many threats are simply forms of crime, espionage, fraud, and activism that make use of the digital domain (Anderson et al. 2012).

Threats may emanate from actors that can be broadly distinguished by five factors: their target, expertise, resources, organization, and motivation (Bruijne, Eeten, and Pieters 2017). Groups of threat actors defined by the National Coordinator for Security and Counterterrorism of the Netherlands (2018a) are criminals, nation-states, terrorists, hacktivists, insiders, and script kiddies. While sharing information impacts each of these actors differently, this study treats threats as a single category.

2.1.1 Practice of threat detection

An organization may institute a Security Operations Centre (SOC) that performs the functions to address a cybersecurity threat: to manage risk, to develop safeguards, to detect the occurrence of events, and to respond to and recover from an event (NIST 2014).

In practice, all four functions could be performed by a single security specialist or entire teams may be dedicated to the various functions. These diverging 'maturity levels' of organizations in terms of their cybersecurity capability are confirmed in the case study research in Section 4.3.1.

An organization may have various preventive threat detection measures side by side. The most common is the firewall, which forms a barrier between an organizations internal network and an external network. A firewall performs shallow inspection of traffic in order to detect threats by looking at packet headers, and dropping the packets when it finds evidence of an attack.

A firewall may be complemented by an Intrusion Detection and Prevention System (IDPS) which is located inside an organization's network rather than at the edge. This system, by contrast, inspects not only the headers but also the contents of traffic on the network. An IDPS system detects malicious traffic by looking for properties of known threats, which are referred to as Indicators of Compromise (IoCs) or indicators for short. Depending on its configuration, an IDPS passively detects and notifies of possible threats or actively blocks possibly malicious traffic flows.

A less common type of systems are honeypots, passive systems that imitate targets of attackers. Since they don't actually serve users, they trigger an event when they are accessed.

Events from an organization's threat detection systems are collected in a Security Information and Event Management (SIEM) system where analysts may examine them and determine how to respond. In addition, analysts may look at historical data in order to identify threats. In the case of the NDN, organizations use a combination of the above, depending on their maturity level.

Problematic of the indicator-based approach is that the evidence it finds of an attack is probability-based. An IDPS therefore generates events in the SIEM that must be validated to be true-positives by human analysts. This can cause a burden to the

organization. Novel types of intrusion detection systems are being developed which use predictive analytics to monitor for events (Patcha and Park 2007; Mahmood and Afzal 2013). While predictive systems may use the same cybersecurity information for learning as indicator-based systems, they are not the subject of this study.

2.1.2 Intelligence cycle

In order to create signatures with which to conduct detection, data on threats must be collected and transformed into actionable information or 'intelligence'. Based on the classic six phases of the intelligence process according to the the (Joint Chiefs of Staff of the United States 2017), cybersecurity firm Mandiant proposes a threat intelligence process lifecycle (Compton 2017). It describes threat intelligence activities in five phases:

1. *Planning & requirements*, definition of requirements of the program;
2. *Collection & processing* of raw data;
3. *Analysis* and interpretation of information against program requirements, and identification of gaps in collection;
4. *Production* of threat intelligence products, like reports or IoCs; and
5. *Dissemination & feedback* of threat intelligence products.

The outcomes of this cycle may take many forms: there is no universally accepted definition of Cybersecurity Threat Intelligence (CTI) and the term is used inconsistently in grey and academic literature. Similarly, no clear definition exists of the technologies that support the collection and exchange of threat intelligence (Sauerwein et al. 2017).

So where exactly in the cycle is the 'intelligence' created? Is this in processing data, in analysis, or in the creation of products? It is hard to say. An overview of concepts around threat intelligence of increasing sophistication is presented in Table 2.1.

Threat intelligence concept	As defined by Brown, Gommers, and O. Serrano (2015)	As defined by Burger et al. (2014)
Indicators	Actionable, spanning many levels and time-scales	Observable patterns or behaviors that indicate that an incident has occurred
Intelligence	Acquired or inferred through analysis, requires decision-making	Action, query, target
Situational awareness	N/A	Who, what, when, where, why

Table 2.1: Conceptual mapping of threat intelligence definitions

Authors Brown, Gommers, and O. Serrano (2015) distinguish between low-level information that is immediately actionable and may be processed in automated fashion, and complex intelligence that has been derived from analysis but requires human decision-making to become actionable. The first are simple data points, the latter may be contained in for example a report.

On the other hand, authors Burger et al. (2014) emphasize that currently in practice, the focus of threat intelligence is on the indicator level. They propose a model of five

layers. They add a macro level that describes the 'situational awareness' which may be gained from threat intelligence. Not pictured in Table 2.1 are the two underlying Session and Transport layers which these authors propose.

As no single definition of threat intelligence exists, authors use different dimensions to distinguish between levels of cybersecurity information. While Brown, Gommers, and O. Serrano (2015) focus on the practical *role* of the information in the detection process, Burger et al. (2014) consider what the data *describes* to determine its level. These authors also discuss an extensive list of data types.

For cybersecurity information in a broad sense, authors Laube and Böhme (2017) distinguish three types: *attack information* on threats and vulnerabilities, *control information* on measures that may prevent or detect an incident, and *impact information* on the assets and losses that were impacted by the incident. Here threat intelligence can once again not be clearly classified: intelligence on threat actors falls in the *attack* category, while threat indicators are part of the *control* category.

Regardless of the definition of threat intelligence, the role of the knowledge of the analyst in detection of threats should not be underestimated. In a study among 55 university students and 20 security professionals, Ben-Asher and Gonzalez (2015) found significant difference in classification performance between the groups for the detection of malicious network events. Even experts who had no professional experience with this performed significantly better than a group of students, which the researchers attributed to the experts' ability to interpret the description and context of events due to their domain knowledge.

This study takes 'cybersecurity threat intelligence' to cover all three layers of Table 2.1: the term covers both the indicators, intelligence derived from this, and situational awareness it may achieve. Where relevant, a distinction will be made between the layers.

2.1.3 The STIX taxonomy

The concept of 'threat intelligence' can perhaps best be understood from how it is operationalized in practice. Since 2011, a number of taxonomies have been developed to express concepts relevant to cybersecurity information. These standards have become the basis for the analysis and exchange of threat intelligence, most notably the comprehensive Structured Threat Information eXpression (STIX) format that was released in 2013 by the MITRE corporation. Due to its wide compatibility and inclusion in many threat detection platforms, STIX can now be considered the de-facto industry standard (Burger et al. 2014; Fransen, Smulders, and Kerkdijk 2015; Sauerwein et al. 2017).

The STIX taxonomy allows analysts to define indicators. An example data point might be an IP-address known to be serving malware which targets a certain vulnerability. Together indicators can enable identification of a malware campaign and the corresponding threat actor. These relationships are displayed in Figure 2.1. In this way, a number of campaigns might be tracked for a threat actor. All concepts in the architecture and their relationships can be referenced in Appendix B.

Indicators that have been formalized in one of the signature formats that STIX is compatible with (e.g. Snort or YARA) can be used for detection by an organization by importing them into their IDPS.

Standards allow organizations to share threat intelligence information. The benefits and challenges associated with sharing will be discussed in Section 2.2. An example of a technology that enables sharing is the TAXII link layer standard, which is coupled to the STIX taxonomy. It formalizes various sharing models: organizations can communicate peer-to-peer, or in a hub-and-spoke, publish-subscribe model. In the latter two configurations, a central organization takes the role of a clearinghouse and may filter the CTI delivered to the other organizations (Burger et al. 2014; Fransen and Kerkdijk 2017).

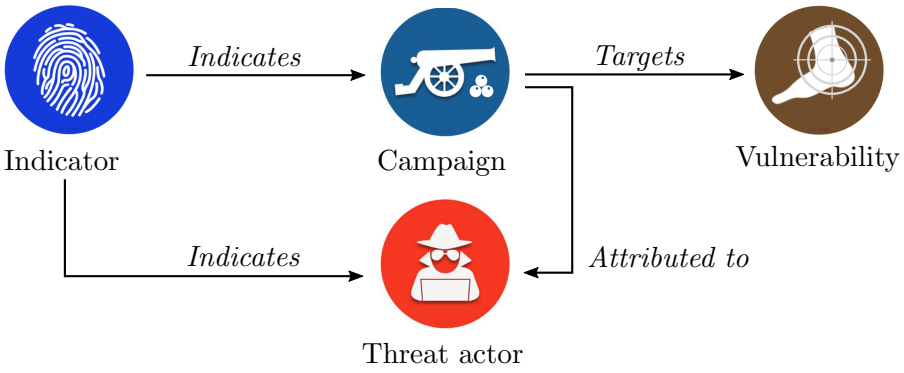

Figure 2.1: Example of relationships between STIX 2.0 objects

2.1.4 Detection capability levels

Cybersecurity threat detection capabilities build on each other. Recall that Fransen and Kerkdijk (2017) distinguish four strategies with which organizations develop resilience: to institute simple controls, to monitor for attacks, to anticipate attacks using threat intelligence, and to automate the response and recovery process. The use of cybersecurity information is suitable for more mature organizations.

Similarly, building capability involves interaction with peers who are using cybersecurity information. NIST (2014) distinguishes four tiers of sophistication in managing cybersecurity risk, not limited to detection capabilities. In each tier, the role of external participation in addressing risk grows. At the highest level of sophistication *organizations share information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.* It must be noted that the authors emphasize that the tiers are not maturity levels, and argue that although progressing to higher tiers is encouraged, this should only happen when it is a cost-effective way of reducing risk.

2.2 Information sharing

The activities described for detecting cybersecurity attacks are currently performed mostly within individual organizations; there is little cross-organizational information-sharing. However in order to understand threats, information sharing is crucial (Skopik, Settanni, and Fiedler 2016). As not every organization has the capacity to independently carry out the activities of the intelligence cycle and develop threat intelligence, organizations can benefit from mutually sharing threat intelligence (Sauerwein et al. 2017). In this way, organizations can improve their security level by making use of the knowledge, experience, and capabilities of their peers. This allows *one organization's detection to become another's prevention* (Johnson et al. 2016). Benefits and risks of sharing intelligence will be further discussed in Section 2.3.

Authors (Skopik, Settanni, and Fiedler 2016) point to the exception of national Computer Emergency Response Team (CERT)[1] as organizations that already do engage in information sharing. This role of the NCSC, the CERT of the Netherlands, in promoting information sharing is exactly the subject of this study and will be explored in Chapter 4.

[1]Some authors make a distinction between CERTs and CSIRTs, or Computer Security Incident Response Teams. No such distinction is made in this study.

2.2.1 Communities of practice and ISACs

Cybersecurity information sharing is often achieved in practice through ad-hoc and informal relationships (Skopik, Settanni, and Fiedler 2016). When security experts exchange knowledge around a shared professional interest, like a cybersecurity threat they are faced with, this may be seen as a community of practice (Wenger and Snyder 1999) in order to better understand the nature of the sharing relationship. Such communities are different from formalized groups and project teams, in that knowledge sharing is the primary output and membership is flexible. Such communities operate under basic rules of conduct, rather than formalized rules (Johnson et al. 2016). An overview of characteristics of three forms of organization is presented in Table 2.2.

An example of a community of cybersecurity professionals with shared interests and engaging in knowledge sharing is the group of European Government CERTs (EGC). This loosely-structured group of arose out of a need by government experts to share information. Members meet three times per year, and communicate over mailing lists and messaging channels (Clark et al. 2014).

Form of organization	Community of practice	Formal work group	Project team
What's the purpose?	To develop members' capabilities; to build and exchange knowledge	To deliver a product or service	To accomplish a specified task
Who belongs?	Members who select themselves	Everyone who reports to the group's manager	Employees assigned by senior management
What holds it together?	Passion, commitment, and identification with the group's expertise	Job requirements and common goals	The project's milestones and goals
How long does it last?	As long as there is interest in maintaining the group	Until the next reorganization	Until the project has been completed

Table 2.2: Characteristics of communities of practice and other forms of organization, taken from Wenger and Snyder (1999)

Formal forms of organization have been developed to structure cybersecurity knowledge sharing. Here participants may be vetted and exchange of information may be subject to Service Level Agreements (Johnson et al. 2016). A notable example of a formalized structure are Information Sharing and Analysis Centers (ISAC). These are trusted fora for sharing information and experiences, often specific to a business sector (Clark et al. 2014; Boeke 2018).

An example is the global Financial Services ISAC (FS-ISAC) that has existed since 2013 and in which banks and other financial institutions participate. They share threat indicators, vulnerabilities, and incidents. A group of analysts validates threat information and shares this with the participants. Similar to cybersecurity communities, ISACs often use fairly simple means of communication. However, the FS-ISAC has taken up the use of an automated threat intelligence platform (Fransen and Kerkdijk 2017). The role of such platforms is further considered in Section 2.2.4.

The government of the Netherlands has set up ISACs for vital sectors of Dutch society, like energy and telecommunications. Participation is voluntary and the NCSC takes only a

facilitating role: organizations together decide on the agenda (Boeke 2018). According to Clark et al. (2014), this participatory approach is influenced by the country's negotiative style of decision-making ('poldermodel').

2.2.2 Community trust

Trust may be seen as an "antecedent to knowledge sharing in virtual communities of practice" (Usoro et al. 2007). Especially potentially sensitive threat intelligence sharing is aided by a level of trust among participants in a community, be it a community of practice or a formalized structure like an ISAC. Over time, certain practices have been established into institutions[2] that improve this trust among participants.

A prime example is the Traffic Light Protocol (TLP) which specifies sharing restrictions on information. Colors are used to denote how information can be further shared (Johnson et al. 2016). Restrictions are formulated as follows, with more detailed prescriptions available:

- TLP:RED Not for disclosure, restricted to participants only.
- TLP:AMBER Limited disclosure, restricted to participants' organizations.
- TLP:GREEN Limited disclosure, restricted to the community.
- TLP:WHITE Disclosure is not limited.

Furthermore, authors Fransen and Kerkdijk (2017) formulate four organizational factors related to trust that determine if a community is likely to offer value to its participants in the long term. First, objectives and focus should be clear: the community should determine the focus of the information they wish to exchange. Second, conditions for membership should be established, as this determines how far parties will be extending their trust. Third, legal constraints on one or more of the participants can bound the confidentiality agreements, for example Freedom of Information Acts, and should therefore be addressed. And fourth, a governance model needs to exist for planning and decision-making.

Besides organizational factors, trust may be aided by technology. The field of privacy enhancing technologies is promising for offering solutions towards information sharing without parties having to trust one another, or between 'semi-honest parties' as it is known in cryptography. Technologies range from simple aggregation to the sophisticated secure multi-party computation, which may come at different levels of informational loss and performance costs (Jongsma and Hoepman 2015; Kamp et al. 2016; Fuentes et al. 2017). Currently such privacy enhancing technologies are not yet being used in practice in widely adopted sharing platforms, such as those discussed in Section 2.2.4.

2.2.3 Intelligence sources and data quality metrics

Threat intelligence is often acquired from multiple sources, depending on the threats an organization expects to face. A wide variety of sources exists, varying from freely available online to coming at a price.

From the perspective of an organization consuming threat intelligence, four categories of sources may be distinguished. First, organizations can develop their own intelligence. As this intelligence is situated in the context of the organization itself, it is potentially highly relevant (Johnson et al. 2016). Second, information is shared by other parties in trusted communities. Third, open source feeds are freely available online, possibly

[2]Institutions in the sense of formal or informal rules which govern behaviour (Ostrom 1990), i.e. not limited to government organizations.

pertaining to certain types of threats. And fourth, commercial feeds are composed by analysts at companies like FireEye, CrowdStrike, and AlienVault (Brown, Gommers, and O. Serrano 2015; Fransen and Kerkdijk 2017).

Except for the case of open source feeds, there is some cost attached to collecting the intelligence, either financially or in terms of a responsibility to reciprocal sharing in a community. Therefore, it becomes important to attach some value to intelligence exchanged in a community or collected from a (commercial) feed. The field of metrics for threat intelligence is still very much in development.

Indicators may be evaluated using the cost or effort they impose on an attacker. Described in grey literature by Bianco (2014) is the 'pyramid of pain' model, which considers levels of indicators by how much 'pain' they inflict on the operation of the attacker if he is forced to adapt. For an attacker it is trivial to change elements of an attack in the lower layers, for example by moving their Command and Control server regularly. It is however more difficult for an attacker to change their Tactics, Techniques and Procedures (TTPs) as these take time to develop, and therefore the value of this cybersecurity information becomes higher. TTPs might include example the language or architecture used in the malware. Going up in the pyramid therefore hierarchy increases the cost to attackers

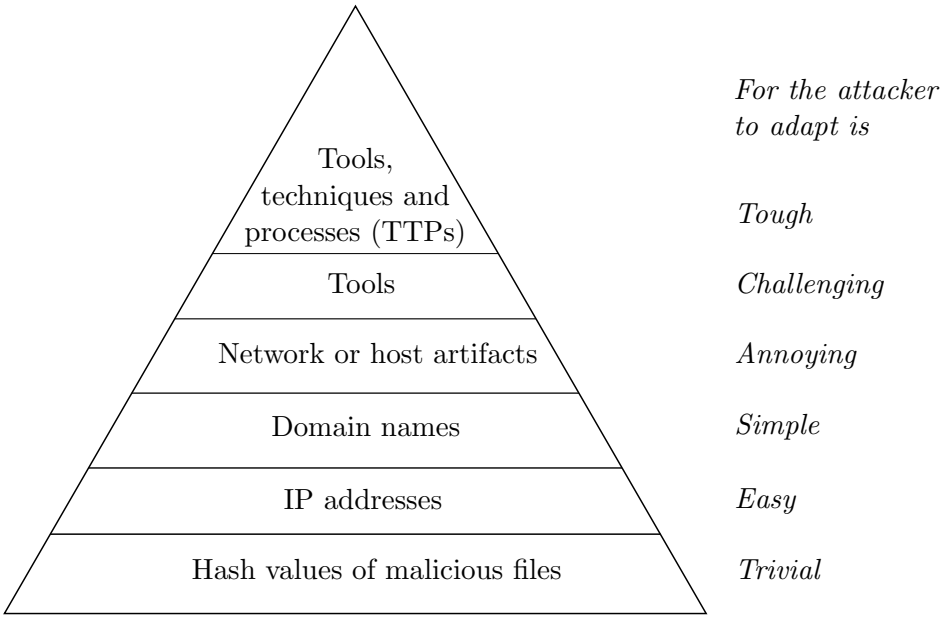

Figure 2.2: Pyramid of pain, adapted from Bianco (2014)

A recent effort by authors Meier et al. (2018) formulates that an ideal threat intelligence feed should be complete, accurate, and fast. Complete, meaning that all relevant indicators should be contained in it. Accurate, meaning that no indicators are listed for benign hosts (false positives). And fast, meaning that it contains information when it is relevant and no longer than this time. Based on these factors the authors design an algorithm to rank threat intelligence feeds. They posit that their algorithm enables organizations to select feeds that contain the maximum amount of distinct indicators, and which list entries before they appear on other feeds. Although the algorithm of Meier et al. (2018) considers completeness of a feed, it does not attach value to indicators, for example based on the pyramid of pain model.

2.2.4 Threat intelligence platforms

Automation of the information sharing process could decrease barriers to sharing and increase the quality of knowledge being shared (Dandurand and O. S. Serrano 2013). To facilitate the exchange of information in cybersecurity communities, platforms have been developed that facilitate this. First in 2013, Dandurand and O. S. Serrano (2013) formulated the following three requirements for such a platform: to facilitate information sharing, to enable automation of this exchange (i.e. by offering an interface to SIEM or IDPS systems), and to facilitate generation and analysis of data. Building on this, authors Brown, Gommers, and O. Serrano (2015) formulated requirements for a system that would go further than facilitate information sharing and enable threat management. An interview with the first author of this article may be found in Appendix A.3.5.

Three years later, a systematic review of 22 threat intelligence platforms was conducted by Sauerwein et al. (2017). Looking at use cases, intelligence sharing functionalities, and collaboration capabilities, these authors conclude that a common definition of threat intelligence platforms is still missing. Findings of Sauerwein et al. (2017) are as follows. The authors conclude that STIX has become the de-facto standard taxonomy for describing threat intelligence. However, current platforms use chiefly the *Observable* and *Indicator* concepts, while the STIX taxonomy offers more concepts that can be used to express higher-level relationships, as illustrated in Appendix B. The authors find that current platforms focus mostly on data collection; the current state of the market for these platforms is described by the authors as 'data warehouses'. The authors find that the bottleneck of the system is often the user, as manual input of analysts is needed to for example determine the sensitivity of information before sharing.

The majority of the platforms is closed-source, and Sauerwein et al. (2017) find that trust issues between users and platforms are mostly neglected. When controls are offered, they are often limited to group-based access control and ranking mechanisms. Governance for sharing in such platforms will be addressed in this study. In the case study of Chapter 4, a threat intelligence platform will be considered more in-depth. Finally, the authors find that academic and commercial interest into threat intelligence has been increasing: they find that the total number of publications on the topic in 2015 was threefold the amount in 2014.

2.3 Individual versus collective rationality

Now having a better understanding of the means of cybersecurity information consumption and sharing, this section discusses the individual incentives and disincentives of sharing threat intelligence. It then considers collective outcomes of sharing threat intelligence, and explores if this results in the creation of a 'public good'. If so, does taking the view of collective rationality lead to higher collective benefits? In order to achieve this, the section lists some design strategies for collective action, and considers if these may be applied to cybersecurity communities. This leads to the identification of a knowledge gap in the final section of this chapter.

2.3.1 Incentives of sharing

In general, there is a role for information sharing in cybersecurity: the question is *not* if information sharing is helpful. As will be shown later, the question is rather how parties can overcome their individual interests in order to benefit collectively. Participation, cooperation and knowledge sharing should be part of any approach for long-term cybersecurity resilience (Clark et al. 2014) and Heuvel and Klein Baltink (2014).

The benefits of knowledge sharing for detection of vulnerabilities arise from the fact that peer organizations may face the same threats. Sharing knowledge about cybersecurity incidents is believed to increase the overall security level by allowing members of a community to take preventive steps (O. Serrano, Dandurand, and Brown 2014; Fransen, Smulders, and Kerkdijk 2015; Brown, Gommers, and O. Serrano 2015).

For sharing threat intelligence specifically, Johnson et al. (2016) describes how sharing enables organizations to use resources that would otherwise be unavailable to them. The authors distinguish four benefits for an individual organization of sharing cybersecurity information.

1. *Shared situational awareness.* By sharing knowledge, experience, and analytic capabilities of peers, organizations can enhance their defensive capabilities;

2. *Improved security posture.* Organizations can inform their cybersecurity and risk management practices using shared information. This allows them to better prevent or respond to incidents;

3. *Knowledge maturation.* Collaboratively enriching information allows organizations to improve the value of their data and provide insights that would otherwise remain unavailable. This can be achieved by sharing sightings on indicators, or cross-referencing data; and

4. *Greater defensive agility.* Organizations may benefit from economies of scale and increase their operational tempo. Although attackers can rapidly adapt their tactics, cooperation allows defenders to raise the cost for attackers by forcing them to continually develop new tactics.

In addition to improved resilience, there may also be a financial incentive to engage in information sharing. The economic model of Gordon, Loeb, and Lucyshyn (2003) shows that economies of scale apply to cybersecurity information sharing: when information is shared in a cybersecurity community, this leads to a higher security level for the participants, even though they need to spend less on their security activities. However, there must be an incentive mechanism in place to realize this potential, as will be discussed in Section 2.3.3. Gal-or and Ghose (2005) describe that organizations can use their participation in an ISAC to signal to customers their dedication to security, arguing that this could increase sales. The authors argue that similarly, participation in an ISAC may act as deterrent to attackers.

2.3.2 Disincentives of sharing

There are risks attached to sharing cybersecurity information for individual organizations. According to Kamp et al. (2016) it is "broadly recognized" that sharing security information can have negative consequences. This is why sharing mostly takes place between parties that already have a high level of trust (Jongsma and Hoepman 2015). Authors broadly consider risks of sharing in three categories.

First, an increased attack surface. Sensitive information might reveal countermeasures to attackers, or result in loss of sensitive data. These could include personally identifiable information or proprietary business data, such as intellectual property (Jongsma and Hoepman 2015; Kamp et al. 2016). Trust in the infrastructure is an important factor in this, according to Fuentes et al. (2017).

According to Albakri, Boiten, and De Lemos (2018), the possibility of disclosure of sensitive information forms indeed the largest perceived risk of cybersecurity information sharing. For the elements in the STIX taxonomy, they conduct a review of the potential

risk of information disclosure, finding to be the highest: the severity of disclosure of the impact on the target, and attribution to an attacker.

Second, compliance issues. For the case of a community with government partners, Kerkdijk and Koens (2017) discuss the risks of () legislation revealing sensitive information to the public. Authors Albakri, Boiten, and De Lemos (2018) posit that laws can both "encourage and inhibit" information sharing. An example of the latter is the barrier formed by having different data protection regimes.

Third, reputation damage as a result of the two above risks (Kamp et al. 2016). This is supported by a 2002 survey among IT executives cited by Gal-or and Ghose (2005), who conclude that diminished customer confidence due to releases of sensitive information could harm their revenues. The risk of reputation damage affecting revenues was of greater concern to the executives than direct harm to their infrastructures.

2.3.3 Cybersecurity information sharing as a collective action problem

If participants in a cybersecurity community operate primarily out of self-interest, they will share little threat intelligence that is of value. This is because sharing information about threats and incidents on their networks puts organizations in a vulnerable position, considering that information about incidents could lead to risks in terms of reputation or compliance for them, or reveal their security capabilities to potential attackers (Kerkdijk and Koens 2017; Fuentes et al. 2017).

However, when peers do collaborate, the entire community benefits. If participants in a community share information, the overall detection capability among organizations improves and the community security level increases. Interests in a cybersecurity community must be aligned and trust between the parties must be especially strong for the sharing of the more unique and sensitive indicators to occur.

Willingness to engage in information sharing sharing may be seen as leading to the creation of a public good in a cybersecurity community. The *free rider problem* in economics is related to the *prisoner's dilemma* in game theory and the *tragedy of the commons* in social sciences. These are problems because the behaviour of rational actors in these situations does not lead to the collective results with the highest value for the actors: individual rationality leads to collective irrationality. Together these three scenarios shape our understanding of property rights and collaborative behaviour (Poteete, Janssen, and Ostrom 2010).

When actors in such situations do manage to collaborate in order to achieve their common interests, this is known as collective action Olson (1965). Organizations in a cybersecurity community setting aside their individual interests in order to share knowledge and increase community benefits may be seen as as a collective action problem.

Solutions to these problems exist. How interactions between participants in a cybersecurity community should be structured to achieve this depends on the type of good that is being created, which is determined by the factors of rivalry and excludability. Rivalry concerns if consumption of the good prevents others from enjoying it. Excludability means if parties can be prevented from enjoying the good (Hollingshead, Fulk, and P. Monge 2002; Poteete, Janssen, and Ostrom 2010).

For cybersecurity information sharing, Gordon, Loeb, and Lucyshyn (2003) show that economies of scale can be achieved if organizations share information in a community. However, the model of these authors also shows that due to the individual risks attached to sharing information, each participant will be motivated to renege on their sharing responsibilities or otherwise provide less information to other participants in the community, while still reaping individual benefits. The authors hereby identify a free rider problem, where participants can enjoy the benefits of a resource (i.e. threat intelligence in the community) without contributing to it (Groves and Ledyard 1977). In this way, individual

	Excludable	Non-excludable
Rival	Private goods	Common-pool resources
Non-rival	Club goods	Public goods

Table 2.3: Types of goods, based on Poteete, Janssen, and Ostrom (2010)

rationality of the participants may lead to collective irrationality in the community (Olson 1965).

According to Gordon, Loeb, and Lucyshyn (2003), this situation would result in the underinvestment in cybersecurity activities in the community. Therefore sharing incentives need to be put in place in order to realize both individual and collective benefits for participants in a cybersecurity community. According to the authors, organizations are unlikely to share sensitive information unless mandated or motivated to do so.

Similarly, He et al. (2016) describe that for cybersecurity investment in general (i.e. not limited to information sharing) organizations are likely to minimize their private costs, which leads to an overall suboptimal cybersecurity level. According to the authors, there is a general consensus in economics literature that that cybersecurity risk is a result of distorted incentives, network externalities, and moral hazard.

Although there is general agreement in literature that cybersecurity information sharing has misaligned incentives, there is no consensus about how sharing information should be characterized or what the type of allocation problem is exactly. There are a number of possible interpretations, depending on how authors define the good of interest, and how the factors of rivalry and excludability are formulated.

Hollingshead, Fulk, and P. Monge (2002) characterize knowledge sharing in an intranet as a public good, as they see it as non-rival and non-excludable "to the relevant public" – without specifying how this group could be determined. The authors suggest mechanisms to deal with the free rider problem for knowledge sharing in intranets.

Shiffman and Gupta (2013) argue that sharing cybersecurity information results in a common-pool source: although they consider the communities to be able to exclude participants (and therefore create club goods), they posit that such communities cannot be seen as separate from the internet in a broad sense. They argue the internet to be a common-pool resource (despite listing a number of key differences), and therefore consider cybersecurity information sharing as also resulting in the creation of a common-pool resource.

In the context of international relations, Hansel (2013) distinguishes a free-rider problem for cybersecurity knowledge sharing between nations. The author expresses that security resulting from sharing knowledge is "probably not" a public good, but rather considers the lack of such knowledge sharing a 'public bad'. He points to positive externalities resulting from states sharing cybersecurity knowledge, as capacity building reduces abuse of networks for harming third parties. The author does not consider it problematic that the good of interest lacks purity, and discusses solutions without establishing the type of good at hand.

Perhaps the factors of rivalry and excludability do not suffice to express the outcomes of information sharing. For ICT networks in a broad sense, authors Fulk, Kalman, and P. R. Monge (1996) conduct a review of works around the concept of public good and extend the concept to *connective and communal public goods* in order to characterize ICT networks. Similarly, Hippel and Krogh (2003) and Weber (2000) argue that the dichotomy between rival and non-rival goods is insufficient by pointing to the positive network effects

of collaboration for open-source software. Weber (2000) proposes to add 'anti-rival' goods, in which their value increases as more people use it. This is related to the concept of positive network externalities or network effects.

Fifteen years ago, Gordon, Loeb, and Lucyshyn (2003) showed the existence of a free-rider problem in the sharing of cybersecurity information. With varying degrees of intellectual flexibility, authors have attempted to address the issue. We should consider if the theoretical underpinning of possible solutions is as relevant as working towards a solution. Similar to the approach of Hansel (2013), perhaps the characterization of the type of good at hand is less relevant than offering solutions to address the incentive problem. Collective action for cybersecurity information sharing has become especially pressing now that communities exist that are sharing threat intelligence in practice, with the technologies described in the first part of this chapter. This study accepts the existence of a collective action problem in cybersecurity information sharing without specifying which type of good is being created exactly. Instead, solutions in the broader field of collective action are considered.

2.3.4 Design for collective action

This section describes principles for structuring interactions in order to achieve collective action. These come from the fields of economics and social sciences. What happens when we analyze cybersecurity information sharing using collective rationality, rather than individual? What avenues for increasing collective benefits can be determined?

To govern a common-pool resource and prevent free-riding behaviour, Ostrom (1990) proposes eight design principles:

1. The community has clearly defined boundaries and can effectively exclude unentitled parties;
2. The resource environment and its governance structure are aligned;
3. Decision are made through participation of parties affected by them;
4. Higher-level authorities recognize the rights of parties to self-govern;
5. Rules are enforced by parties who are accountable to the community;
6. Violations are punished with graduated sanctions;
7. Conflict resolution mechanisms exist that are low-cost and easy to access; and
8. In large communities, rules are organized and enforced in layers of nested enterprises.

These principles were extended in later work by Poteete, Janssen, and Ostrom (2010) to include communication, internal trust and reciprocity. Many exist in this field.

Based on a 'network approach' to governance theory, Dunn-Cavelty and Suter (2009) argue that the protection of critical infrastructures should rest on self-regulating and self-organizing networks. The governments role in this should be to coordinate the networks and identify instruments that can help motivate networks to meet the shared responsibility of protecting critical infrastructures. As will be argued in the following chapters, this perspective is relevant to cybersecurity information sharing as well.

Meaningful interactions in a community are harder to achieve using a virtual system, according to Shiffman and Gupta (2013) in their reflection on open source cybersecurity. This makes building trust relationships when sharing also difficult. Based on these authors' perspective on the internet as a 'commons', they propose that central authorities should "provide a space where security experts can build trust relationships that foster

coordination and communication". The authors do not specify how this space should be achieved. Contributing to this challenge is the aim of this study.

2.4 Knowledge gap

Collective benefits may be achieved by sharing information in a cybersecurity community (Sauerwein et al. 2017; Johnson et al. 2016). A 'free rider problem' in sharing cybersecurity information was established fifteen years ago, and the need to design incentives for information sharing in vital sectors thirteen years ago (Gordon, Loeb, and Lucyshyn 2003; Gal-or and Ghose 2005).

Recent contributions attempting to improve trust in cybersecurity communities focus on technology and do not address the issue of misaligned incentives (e.g. Jongsma and Hoepman (2015), Kamp et al. (2016), Fransen and Kerkdijk (2017), and Fuentes et al. (2017)).

Theories using public goods and collective action have been developed for knowledge sharing in communities of practice and in a general ICT context, like intranets (Wenger and Snyder 1999; Hollingshead, Fulk, and P. Monge 2002). For cybersecurity communities however, no such theories exist.

The most relevant work in this area is by Shiffman and Gupta (2013), who propose to "crowdsource cybersecurity". The authors motivate this using their analysis of the internet as a 'commons', and give directions for further research based on theory on collective action. Although the authors discuss the need for detection of threats, they do not consider cybersecurity threat intelligence communities in particular, and the authors do not specify requirements or design principles for the solutions they propose.

A knowledge gap is identified on governance design for collective action problems in theory on cybersecurity information sharing. In the following chapters, this knowledge gap will be addressed through a case study, requirements, and a governance design. In the Conclusions chapter, the contribution will be made explicit.

The first sub-question of the study can now be answered: *What factors determine the level of information sharing in a cybersecurity community?* An organization's detection capability level and corresponding technology and processes influences its consumption and analysis of threat intelligence. The level of information sharing is determined by the individual costs and collective benefits associated with sharing in the community. This can be understood from the perspective of collective action theory, which offers principles for design of solutions.

Chapter 3

Methodology

This chapter addresses how the research question and sub-questions will be operationalized, and considers limitations of the chosen research approach. The research question as formulated in Section 1.2 is: How can information sharing in the National Detection Network be incentivized?

The problem is broken down into subquestions:

1. What factors determine the level of information sharing in a cybersecurity community?
2. Are missing incentives limiting information sharing in the NDN?
3. What are requirements of governance that improves information sharing?
4. How can the NCSC introduce these measures in the NDN?

The research approach is structured using Design Science Research Cycles of Hevner and Chatterjee (2010). An overview of this methodology is displayed in Figure 3.1. The research draws on the knowledge base of collective action and process design, while ensuring relevance for the National Detection Network environment. Requirements of engagement and a governance design are generated that contribute to both. An overview of the research flow is presented in Figure 3.2.

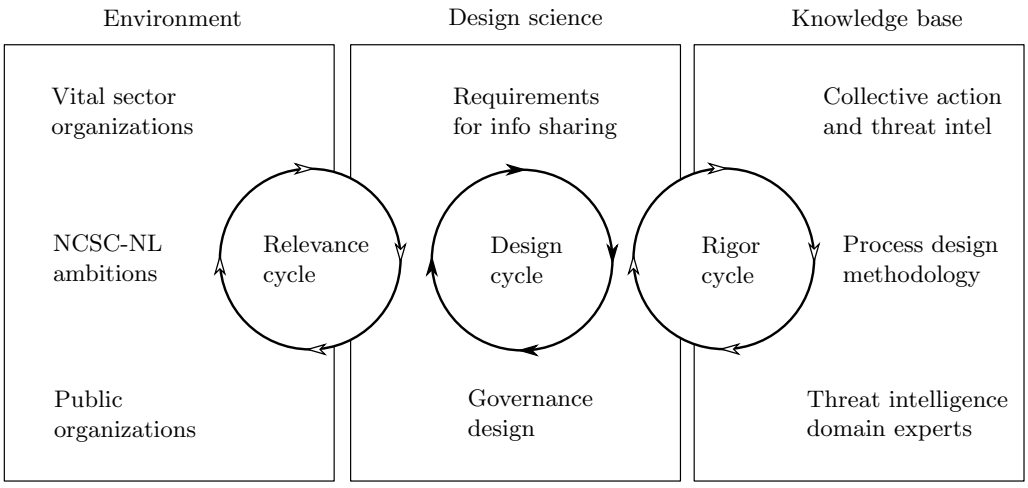

Figure 3.1: The Design Science research cycles for this study, adapted from Hevner (2007)

Through the rigor cycle, the design creates a knowledge contribution. The knowledge base in which the design is founded, is described in the literature review of Chapter 2.

Through the relevance cycle, the design adds to the environment. For sub-questions 2 through 4, the knowledge gathered in the literature review is applied to the environment of the National Detection Network (NDN) of the Netherlands in a case study research to synthesize requirements for engagement in a cybersecurity community. The approach of the case research is described below, while the case description exists in Chapter 4. Sub-questions are answered over the course of chapters 2, 4, and 5.

To address the governance design problem of sub-question 4, the Process Management method for interactive decision-making by Bruijn, Heuvelhof, and 't veld (2010) is used to propose a process. In two iterations of the design cycle, a design for an interactive decision-making process is formulated. The method is elaborated on below in Section 3.2. Answering sub-question 4, the design is described in Chapter 4.

The final two chapters return to the main research question. In the Discussion chapter the requirements and design for the National Detection Network are generalized for other types of cybersecurity communities, and limitations of the approach are discussed. In the Conclusions chapter, the results are placed in the appropriate context.

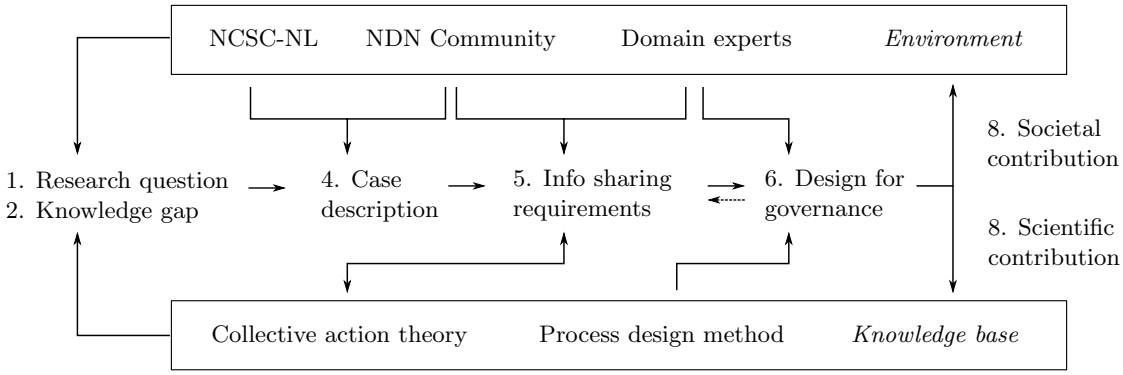

Figure 3.2: Research flow diagram

3.1 Case study research at NCSC

During a six-month internship at the National Cyber Security Centre (NCSC) of the Netherlands, the case of the National Detection Network was examined. This is a cybersecurity community in which public and private organizations exchange knowledge about threats they are faced with. The internship was the result of an open application for thesis research, suggesting the research topic of threat intelligence exchange in the NDN.

The internship at the NCSC enabled access to a diverse group of stakeholders around the NDN. Three groups were identified for a series of 19 qualitative research interviews: system owners (i.e. representatives of the NCSC and the AIVD), the organizations that form the community of the NDN, and experts that could improve and validate the design. Summaries of these conversations are presented in Appendix A. As well as a resource to answer the research question, these interview summaries together form an important output of the thesis project.

3.1.1 Interview selection

Of the system owners of the NDN, two out of three organizations were interviewed: the NCSC and AIVD. This is motivated in Chapter 4. The system owners form the first group of stakeholders. The members of the cybersecurity community form the second. They were previously identified by the NCSC as being part of the 'constituency' of the

NDN: they are either already participating in the NDN, or could potentially participate in a later stage. Which organizations can be part of the constituency is determined by the organizational mission of the NCSC to protect vital sectors. While this was taken as-is for demarcation of the group, the underlying selection criterion is challenged in Chapter 6.

To ensure a diverse selection of NDN community members, both public and private organizations were interviewed, and organizations with a high as well as low level of organizational cybersecurity maturity. The selection of organizations was made together with liaison staff of the NCSC ('accounthouders'), as they formed a trusted link to set up the interviews. While helpful, this introduced the risk of a bias towards community members that had either good pre-existing relations with the NCSC staff, or are already highly engaged in the NDN project and willing to demonstrate their involvement. Just a single organization did not respond to the request for an interview. As is further discussed in Chapter 7, this might confirm the possible engagement bias, while at the same time reducing the risk of self-selection bias.

A third group, consisting of experts, was selected by suggestions originating from the thesis supervisors at TU Delft, as well as NCSC staff. Here the risk of self-selection by the interviewees is higher, as just 9 out of 15 experts responded to a request for an interview.

3.1.2 Procedure and confidentiality

All research results are public, and thesis research contains no confidential addendum. Therefore trust was essential in the interview process. Conducive factors for trust in the interviews were the completed screening process for the internship ("veiligheidsonderzoek B") and introduction through the trusted link at the NCSC. The procedure was communicated in the initial requests for interviews.

The interviews were conversational and addressed the following topics:

1. The value of cybersecurity for the organization, assets to protect and threats to respond to;

2. The organization of the detection capability in the organization, types of threat intelligence used and their sources;

3. The practice of sharing threat intelligence with peers, desired type and form of output of sharing sightings; and

4. Participation in the National Detection Network platform, expectations and experiences, perceived stance of other parties.

All interviews except one were translated from the original Dutch to English. Where deemed relevant, information from the original Dutch was preserved in the interview. As part of the procedure, all interviewees were given the opportunity to check the validity of the summary of the interview and alter how they would be referenced. A minority took the opportunity to make changes, for example to remove details that might allow them or their organization to be identified or harm operational security. During this phase, one expert declined for the summary of the interview to be printed in the thesis and so no conclusions could be based on this interview.

Information learned during the internship at the NCSC could be found to be sensitive. Therefore, NCSC staff were given the opportunity to check the thesis document before publication. No parts of the text were redacted and no conclusions were altered.

3.2 Process design for complex decision making

In the design cycle of the research, a proposal for governance of the National Detection Network is proposed using the Process Design method of Bruijn, Heuvelhof, and 't veld (2010). This method describes how to move from a unilateral, project-management approach to problem-solving in a networked or 'process' approach.

When working towards a common goal in a network of organizations, a governance structure must be designed that builds commitment from the parties. This is how a diverse set of stakeholders with diverging or even conflicting interests can collaborate towards shared goals. The method of Bruijn, Heuvelhof, and 't veld (2010) is not limited to collective action problems, but fits well with the domain.

The method resulted in high-level requirements and a design for an interactive decision-making process for the NDN, with the aim to increase the level of community information sharing.

In the words of Hevner and Chatterjee (2010), this approach to design can be seen as a "search". Requirements from the environment and the knowledge base reinforce the design cycle. Two iterations of the design cycle took place, with interview A.3.8 providing feedback on the initial design. A contribution to the environment exists in the governance design for the National Cyber Security Centre. A contribution to the knowledge base resides in stakeholder interviews and generalized design requirements.

3.2.1 Core elements of a process design

The need for a process approach to the NDN is established in Chapter 6. The steps for the NCSC to move to a network approach of the NDN are then described.

When designing governance in a network of organizations, trade-offs between must be made at the start of the process and when managing the network (Bruijn, Heuvelhof, and 't veld 2010). The Process Design methodology specifies four trade-offs that in turn influence each other: openness, protection of core-values (i.e. achieving commitment), progress, and content (i.e. decision-making quality). These are displayed in Figure 5.1. and used to structure the requirements.

3.2.2 Process architecture activities

Process design is not a mechanistic activity; and it is not necessary to complete all activities in order to arrive at a good process design or carry out activities in a fixed order (Bruijn, Heuvelhof, and 't veld 2010).

With the described trade-offs as design guidelines, a selection of the activities in the process design methodology were carried out. These are described with their background and design choices in the design Chapter 6. In the words of (Bruijn, Heuvelhof, and 't veld 2010) the described elements of interactive decision-making together work towards a desirable "package deal" for all stakeholders of the NDN.

Chapter 4

The National Detection Network

This chapter describes the case study of the National Detection Network (NDN) of the Netherlands, and addresses the question if missing incentives are limiting information sharing in this community. This is the second sub-question of the study.

The system of interest throughout the research is the NDN community in a broad sense: the National Detection Network is not reduced to its technologies and processes in this research, but rather considered as an ongoing cooperation between a diverse group of public and private organizations.

The history of cooperation is described in this chapter and an overview of current systems and measures supporting the community is provided. Based on 19 interviews with participants and domain experts, experiences and interests of the community participants are discussed in order to understand if a collective action problem exists in the NDN community.

4.1 Process history

The National Cyber Security Centre (NCSC) is part of the Ministry of Justice and Security of the Netherlands. In 2013, it started a pilot project for detection of malware threats on government networks in collaboration with with intelligence agencies AIVD and MIVD, respectively responsible for general and military intelligence [A.1.2].

The project was referred to as the 'monitoring network' and later the National Detection Network (NDN). It was staffed with 2,5 full-time employees at the NCSC, which funded and managed the project. The NDN consisted initially of placing a limited number of IDPS systems or 'sensors' at government organizations in order to experiment with privacy-friendly collection of network data by the NCSC. This is still the basis for the current architecture as described in Section 4.2.

The project was also a pilot for information exchange and collaboration between government parties in the Netherlands. The NCSC held expertise and authority but but no formal decision power over other government parties, each of which is independently responsible for their ICT networks. This led the NCSC into the first stakeholder process for the NDN community, over time placing sensors at more organizations and growing the group of participants. In this process, it was necessary to for example reassure various employee councils ('ondernemingsraden') of the privacy safeguards built into the system [A.1.1].

In December of 2013, a parallel process was started to engage private organizations in vital sectors of Dutch society (National Coordinator for Security and Counterterrorism of the Netherlands 2018b). Over a period of a year a series of round-table meetings took place with a group of 8 vital sector organizations. This included financial institutions and organizations in the energy sector. They discussed how a cooperation on threat intelligence

should work and what it should deliver. The private organizations agreed to work towards sharing the information they learned from their own IDPS systems with each other and the NCSC [A.1.1].

At the time the sharing infrastructure (MISP, see Section 4.2.2) did not support a participant sharing events from their network, i.e. when a hit occurred on an indicator received from in the NDN. The NCSC supported the development of this feature and it was implemented in MISP in 2016 (Interview A.3.6 and MISP Project (2017)). Slow progress on the technology led to initially limited value which the private organizations derived from the threat intelligence in the NDN. By pointing to the effects of sensors at the public organizations, the NCSC attempted to demonstrate how by sharing sightings, private organizations could improve situational awareness. Interest had however somewhat faded for the more mature organizations and while no participants exited the NDN, few contributions in terms of sightings or research were made. Section 4.3 further describes participant experiences when sharing.

The sharing of indicators was indicative of the limitations of the open-source MISP tool: useful for exchange of IoCs, but slow in adapting to specific use cases wanted by the NDN community. While the MISP system was suitable to distribute intelligence, features for analysis and enrichment of threat intelligence were not meeting demands. The NCSC began testing the EclecticIQ system in 2016, which for participants became known simply as 'the Threat Intelligence Platform' or TIP. This tool was introduced at government participants in order to meet a demand for collaborative analysis of more high level threat intelligence like TTPs. Meanwhile, private organizations still use the MISP platform. The NDN infrastructure is described in Section 4.2.

Funding of the NDN grew with the Dutch national budget of 2016 and the start of a new government in 2017. This allowed the NCSC to increase the staffing of the project and speed up progress. Currently participating in the National Detection Network are 41 public organizations and 21 private organizations from vital sectors. The goal of the NCSC is to work toward around 300 participants [A.1.1]. As of January 2019, the NCSC will reorganize. The NDN will become a central activity in its processes.

4.2 System description

The National Detection Network is a cooperation between the Ministry of Justice and Security (which the NCSC is part of), the AIVD, and the MIVD. It has three stated ambitions (NCSC-NL 2018). First, to create CTI readiness: "be organized on a national as well as at NCSC level". Second, to increase resilience: "use CTI data and insights for cyber defense". Third, to increase situational awareness: "have an overview of threats and attacks in the Netherlands". To these ends, the NCSC provides four services to participants in the NDN. These activities will be described in the below sections.

4.2.1 Sensors for detection

Public organizations can host an Intrusion Detection System (IDS) that is managed by the NCSC. This physical device resides in the network and is referred to as a sensor, as it monitors network flows that pass through it. It produces a 'hit' when a match is found with a predetermined set of indicators that are delivered by the NCSC. In this case the organization receives a notification, and can choose to share the hit event with the NCSC. Contrary to an IDPS, a sensor does not block traffic straight away.

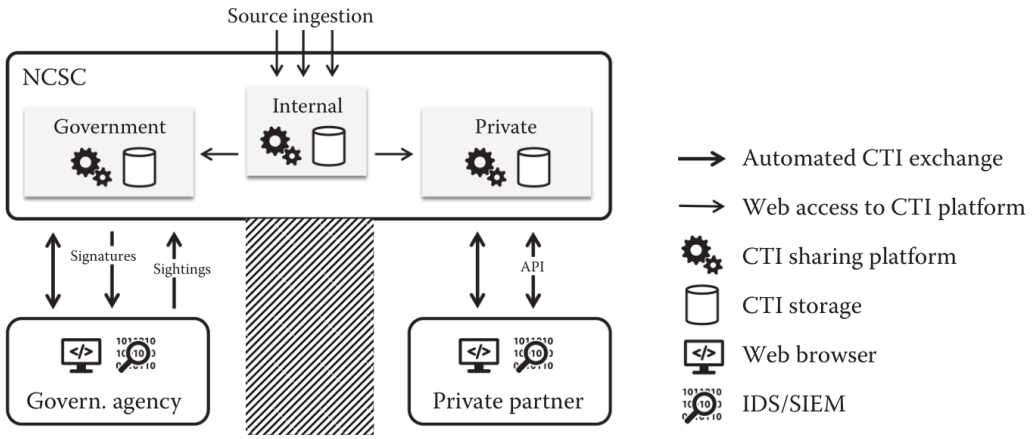

Figure 4.1: Simple schematic of NDN architecture, reproduced from Fransen and Kerkdijk (2017) with permission from the author

4.2.2 MISP for IoC storing and exchange

The Malware Information Sharing Platform (MISP) is open-source software maintained by the Luxembourg CERT. Its focus is on storing and exchanging indicators, as it the case for many contemporary platforms (Sauerwein et al. 2017). Interview A.3.6 with a core developer outlines project governance and roadmap of the MISP project.

MISP stores events that can take the form of many taxonomies (including STIX) which can be extended in free text. When a user creates an event, for example to catalogue a malware sample, they can select one of four sharing levels (Wagner, Dulaunoy, and Iklody 2016):

1. Organization only. Their colleagues will be able to see the event;
2. Community only. Users in the MISP instance will be able to see the event;
3. Connected communities. Users of all MISP instances of the host network of the instance will be able to see the event; and
4. All. Any MISP user can see the event.

The National Detection Network uses three instances of MISP in order to exchange information between participants and collaborate on threat intelligence. One instance serves public organizations, the second serves private vital sector organizations. The third instance functions as a clearinghouse and is proprietary to the NCSC. The NCSC receives intelligence from its (international) partner organizations in this MISP instance before sharing it with the public and private participants in the two respective MISP instances. This architecture is presented in Figure 4.1.

Participating organizations can access the NDN MISP via a web-interface. In addition, they can connect via an API, in order to pull events into their SIEM system and create NDN sightings from within their existing SOC processes. At least one organization has set up its IDPS to start blocking using NDN indicators as soon as they are published, i.e. without analyst intervention [A.2.7].

4.2.3 Threat intelligence shared by the NCSC

The NCSC processes large amounts of cybersecurity data on a daily basis and through analysis derives indicators from this. In addition, analysts at the NCSC gather specific

information to derive high-level threat intelligence that may be shared in forms other than indicators, like management reporting. This section considers the former, which are shared with the NDN participants for (automated) use in their detection capabilities, as well as pushed to the sensors for the case of public organizations. In Figure 4.1 this is described as 'source ingestion', while IoCs are labeled 'signatures'.

The NCSC collects threat intelligence from a variety of sources. Some of these are presented with their approximate distribution in terms of volume in Figure 4.2. However, volume does not imply value: a single unique indicator can result in many hits, or prevent an incident with large impact. The diagram is a one-way simplification of the NDN. Not pictured in Figure 4.2 is information flowing back from participants to the NCSC (and potentially to the original source) when events are enriched, for example through sharing sightings or by adding own research.

1. *Trusted communities*, which include
   - The European Government Certs (EGC) group. This is an informal cooperation of 13 CERTs of European Member States and the European Union CERT;
   - The private sector and global CERT community MISP instances hosted by the Luxembourg CERT that maintains the software. This has become a central place in information exchange;
   - The NATO MISP instance with various NATO members.
2. *Open source feeds, which include*
   - A sinkhole list of domains and IPs that function as DNS sinkholes;
   - The Abuse.ch SSL blacklist of domains that are associated with malware or botnet activities;
   - The Abuse.ch Zeus tracker of domains and IPs that are associated with the Zeus malware; and
   - Unstructured intelligence from open sources, like academic and independent security research.
3. *Research activities* by NDN community members, i.e. analysts at the NCSC, AIVD, MIVD, and participants. While low in volume, these are highly relevant to the context.

As can be seen in Figure 4.2, not all threat intelligence is propagated through the NDN to private organizations, although public organizations receive all information. This is due to the sharing limitations described in Section 2.2.2, which arise mainly from trusted CERT communities in which TLP-Amber information is shared with the NCSC. This can be shared with government organizations but not private organizations.

The NCSC is exploring supplementing these threat intelligence sources with a commercial threat intelligence feed [A.1.1]. Similar limitations on sharing would likely apply to events in such a feed, although it is possible to share intelligence from commercial feeds with third parties, as for example Deloitte shares indicators from a FireEye feed with their customers [A.3.1].

4.2.4 TIP for threat analysis

The EclecticIQ platform is being tested by a group of public organizations in the NDN. The platform supports the analysis and visualization of threat data in STIX format which is synchronized from the public organizations' NDN MISP instance for the duration of

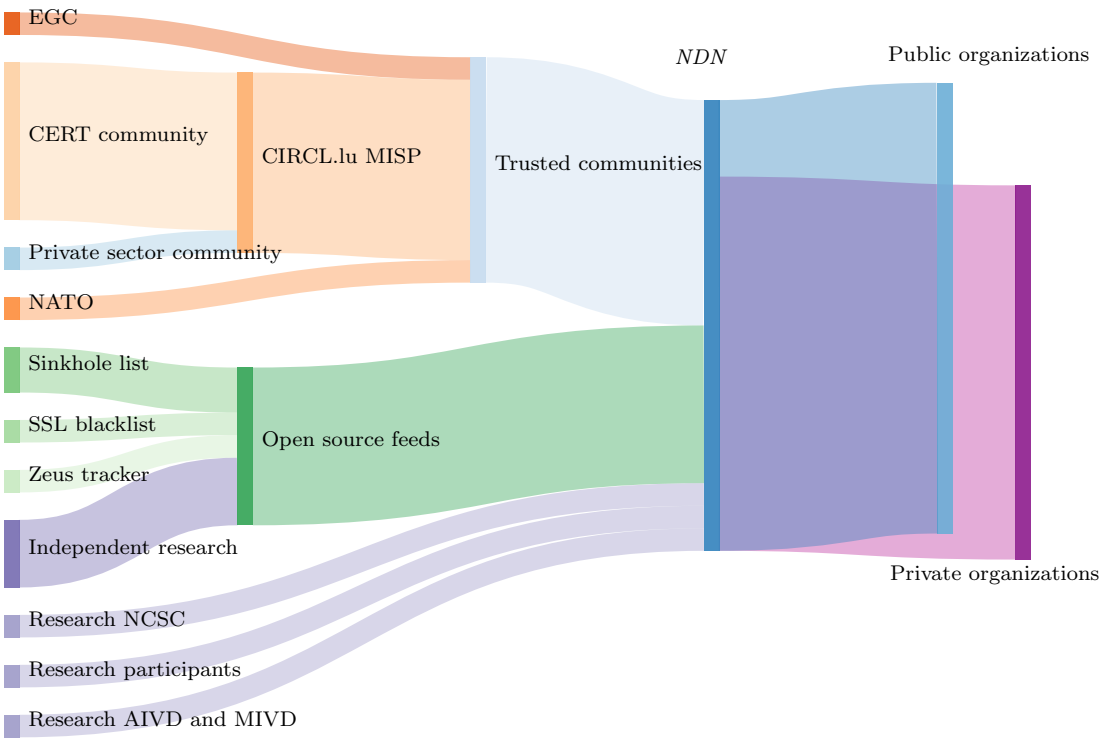

Figure 4.2: Approximate volume of events shared in the NDN by the NCSC, by source

the pilot. The aim is to work toward a system that can supplement the current MISP architecture. The system is now provided as a service to participants, solving problems earlier problems with integration [A.2.8].

4.3 Interviews with system owners and CTI community

This section describes the findings of a series of 19 interviews conducted in the study. Through the interviews, an analysis is made of consumption of threat intelligence by participants in the NDN, their information sharing behaviour, and choices on governance of interactions in the network. One interviewee declined for the summary of the conversation to be printed, therefore no conclusions could be based on it.

Interviews on which this analysis draws are presented in Appendix A, with each citation referring to the number of the source interview in [brackets]. To aid readability, quotes are printed in *italics* instead of in quotation marks for the remainder of this chapter.

4.3.1 Threat intelligence consumption

What do parties want from the National Detection Network? How do organizations benefit from participating in the community and what information are they most interested in obtaining?

Some members of the NDN community formulate cybersecurity as prerequisite to their business processes. Banks relate cybersecurity to the relationship with their customers, stating for example that *the product of a bank is trust* [A.2.3]. Drinking water companies and Rijkswaterstaat name protection of their operational technology and physical assets as being central to their respective missions [A.2.5, A.2.8]. Other organizations view security more instrumental, and have made explicit a level of acceptable risk. A strategic security

specialist at a bank describes: *I'd be satisfied when if NDN manages to help us to reduce risk and stay in bounds of the risk appetite as defined in broad terms for operational risk management in a cost effective manner* [A.2.1].

There is a wide range in participants' cybersecurity maturity levels and corresponding detection capabilities. Whereas a drinking water company 1 has one employee responsible for all ICT security, bank 1 has a team dedicated solely to gathering and analyzing threat intelligence [resp. A.2.6, A.2.1]. In broad strokes one could state that of the organizations interviewed, financial institutions have more mature cybersecurity organizations. This does however not mean that detection capabilities in mature organizations have been fully developed. In 2017 Dutch financials Rabobank, ABN-AMRO and ING were consuming threat intelligence from commercial sources, but stated in joint research that they were *still in the early stages of establishing an effective and sustainable CTI practice* (Kerkdijk and Koens 2017). This data point is corroborated by an interview at a Dutch bank, where an employee states that *threat detection will definitely play a large role in our security architecture, but we are still in the process of determining what we want to do with threat intelligence* [A.2.4].

Organizational cybersecurity maturity therefore influences the role of National Detection Network in detection capabilities. All participants interviewed collect threat intelligence from multiple sources, but depend on the information in the NDN in diverging ways. For drinking water company 2, the NDN is its primary source, going so far as to automatically insert indicators from the NCSC in their IDPS without requiring analyst confirmation [A.2.7]. They do not do this for their other CTI sources, which include open sources. Asked why they value the NDN above other sources, they explain: *The NDN is our primary source for two reasons: validation of information by the Dutch intelligence services ("inlichtingen- en veiligheidsdiensten"). And second, relevance for the Netherlands and vital sector organizations.*

By contrast, for bank 2 the NDN is merely one its threat intelligence sources, besides their security hard- and software vendors and the FS-ISAC community [A.2.3]. The interviewed strategic expert at this organization expressed a desire for higher-level intelligence: *The CTI in the NDN is now very operational, located in the bottom of the pyramid of pain*[1]*. You want it to be higher, in the TTPs. This is more interesting because TTPs are more persistent for an attacker over time, but also because they have a lower false positive rate* [A.2.3]. On the quality of indicators they added: *We expect and indeed see the NDN delivering higher quality data than some of our other sources, where the false positive ratio is so high it becomes hard to extract the relevant information* [A.2.3].

Similar to drinking water company 2, other participants name the involvement of the AIVD and MIVD in the NDN as a means to get access to indicators unavailable from other sources. A strategic specialist at bank 1 described: *The added value of the NDN lies in receiving information that we cannot get from other sources. The first is CTI from intelligence agencies. In the past we've also been asked to exchange CTI with the agencies outside of the NDN, which made this added value less clear. The second is information from sightings reported by other parties in the NDN, which would indicate the urgency of a threat to our organization* [A.2.1]. Here sightings are expected by the interviewee to enrich events to create a level of situational awareness for the bank. Although the added value is described explicitly by the strategic expert at this bank, their colleague prefers to use threat intelligence from commercial sources and mentions that they do in fact *not* use the NDN much [A.2.2].

[1] See the description of the Pyramid of Pain by Bianco (2014) in Section 2.2.3.

4.3.2 Information sharing

Besides consuming cybersecurity information, what is the stance of organizations on sharing it? Participants in the NDN were asked about their motivations to share their research and hit events with peers, and the costs that are associated with this. Conversations were not limited to sharing in the NDN, but also bilaterally or in other forums like ISACs. Organization's stated ambitions were confirmed by asking about specific experiences with sharing.

The private organizations stated preconditions for sharing sightings with the NCSC, like confidentiality and automation in their existing processes [A.2.1, A.2.3, A.2.4] or an improved graphical user interface [A.2.5, A.2.6], the latter participant hoping that *the NDN would become more interactive and lively* if more sharing would occur due to this.

Financial advantages of sharing intelligence were described as follows: *gathering and interpreting CTI could well be done collaboratively, which leaves more resources to focus on the response* [A.2.1]. By others more functionally as: *Because of the NDN we do not need our own team of threat intelligence analysts* [A.2.7].

Some named effectiveness or reducing the rate of false positives as reasons to share intelligence: *Reporting of sightings is an important part of closing the feedback loop. They could be used to increase data quality by validating events. Sightings should also lead to more focus with threats offered that are specifically relevant to the Netherlands* [A.2.3].

Rijkswaterstaat referred to the sharing of threat intelligence as serving a national interest: *I believe the importance of exchanging threat information is evident. It is strongly tied to security of the Netherlands. You have to share in order to advance as a whole* [A.2.8]. Interestingly, the same two NDN participants who described their own financial advantages also referred to collective goals: *Parties in the NDN have achieved a step towards better cooperation: together you can achieve more.* (...) *By sharing CTI we collectively have a higher probability of detecting attacks* [A.2.1]. The other described how it as a vital sector organization benefits from sharing, as it in turn relies on other vital sector organizations for its mission. The organization linked this to a collective goal of improving security: *our organization is dependent on other critical infrastructures: an outage of the electrical grid would for example mean that we could not meet our goal of delivering drinking water. Therefore we should share information between sectors to improve security overall* [A.2.7].

Drinking water company 2 considers itself an ambassador of the NDN, and has a strong drive to in fact *share more than is currently possible. First, we would like to be able to report sightings for hits as well as non-hits, i.e. when we scan for an indicator we want to be able to share when it was not found, as well as when it was found. Second, we want to be able to do this for two sensors: outside our firewall and inside our network. And third, we want to be able to report sightings for indicators coming from sources other than the NDN.* This will be discussed in Chapter 6.

These ambitions to share information are not matched in practice. When it comes to actual usage of the NDN systems, three out of five organizations state problems preventing them from participation. Bank 2 was having an authentication issue with the MISP instance [A.2.4], Rijkswaterstaat was not succeeding in getting the TIP platform operational in their organization[2] [A.2.8], and drinking water company 1 was logging into the MISP web interface *once or twice a month* and not sharing due to complexity of the interface, describing: *The interface makes the system hard to follow, and it is hard to create a new event so that others can actually use it: what boxes to tick, what colors to apply? It would take us a lot of documentation before we could actually contribute* [A.2.6].

The employees of drinking water company 1 found the MISP web interface overly

[2]This issue has since been resolved, as the NCSC started offering the EclecticIQ platform as a service.

complex. The previous NCSC approach for outreach on training and integration of MISP seems not to be reaching them: *During the training there was brief attention given to the fact that an API exists but this lacked practical follow-up* (...) *A more active approach from the NCSC would be welcomed* [A.2.6].

It is interesting to note that the two out of five organizations that had invested in automating the connection with the NDN had no operational issues. About connecting to the API drinking water company 2 remarked: *Already in 2016 we made a real-time connection with the NDN, and were able to do two-way exchange of intelligence. The total initial costs of using the NDN were around €15.000* for this organization [A.2.7].

The two banks interviewed did manage to use the MISP interface to share their information, but noticed a lack of response. Bank 2 remembers: *Some years ago we attempted to share CTI stemming from our own research, but the NCSC did not seem to know what to do with it* [A.2.3], and bank 1 identifies a possible cause after the same had occurred to them: *when sharing CTI in the NDN we have noticed a lack of response. When we shared our own analysis of a previously unknown phishing attack, we did not get feedback from the NCSC or peers. This may be due to overlap with other forums where we share information, in this case a mailing list of peers. Here we did receive feedback.* (...) *It is hard to identify beforehand what type of feedback should be provided by the NCSC* [A.2.2].

So although participants describe their ambitions of sharing information in the NDN, their experiences do not fulfill the promises of information sharing. This is corroborated by the interview with an employee of the NCSC, who states that hits or sightings in the NDN is now primarily being shared by from sensors at public organizations [A.1.1].

4.3.3 Governance expectations

Consuming threat intelligence brings benefits, while sharing comes at a certain cost. How do participants in the NDN perceive the roles of the system owners in promoting information sharing? And how do the NCSC and AIVD themselves view their responsibilities in the system?

Could the benefits of sharing information in the NDN currently be perhaps not sufficiently large to draw mature participants to sharing and responding, instead choosing other platforms for this? About combating a lack of internal support in the organization for sharing CTI in the NDN, a strategic security specialist at bank 1 proposed: *I believe the best to overcome this type of resistance is to have participating organizations show the added value, and through automation reduce the barrier to participating.* However, in the same conversation they describe their recent parallel efforts to also start exchanging information through increased cooperation in a national Finance CERT [A.2.1]. These efforts need not interfere, but it shows that the banks see the value of exchanging threat intelligence and now have an alternative to the NDN to do this.

Three participants call on the NCSC to take an active role in adding new participants to the NDN and helping automate the sharing process [A.2.3, A.2.7, A.2.8]. In addition, organizations express a desire for more open communication from the NCSC. Rijkswaterstaat describes how to them *the NDN is a black box. There is a high level of secrecy at the NCSC and we do not know what are the inputs or outputs of the sensor in our network* [A.2.8].

Both drinking water companies would like more open communication, and offer to become involved and contribute to the NDN. Drinking water company 2 would like to be informed on NDN development: *Our organization considers itself an ambassador of the NDN, but to be honest I could not tell you anything new about the NDN as compared to one year ago. We would like to know the status of the NDN: what is currently the focus of the NCSC, and what is the product roadmap?* [A.2.7] Going beyond staying informed, drinking water company 1 would like to be more involved in the decision-making process

of the NDN: *You don't hear enough about the NDN. We've been to the training, but after that you just receive a lot of system emails and that's about it. I would welcome a more active discussion with other participants maybe once every quarter on problems people are having and the direction of the development of the NDN* [A.2.6] Considering that these organizations have limited organizational capacity devoted to cybersecurity, it is interesting that on top of offering to become involved in decision-making, drinking water company 1 proposes to devote capacity to development of NDN systems: *Decisions about the future of the NDN should happen with a small circle ("en petit comité") of engaged organizations. We would be happy to follow up to these decisions and contribute to development of the platform.*

This research takes the national government perspective on the NDN. A study of the NDN community therefore includes critical assessment of the aims of the NCSC, AIVD, and MIVD with the National Detection Network. They have initiated the community and manage it, and are therefore referred to as the system owners. Chapter 6 considers the implications of this role.

Interviews with representatives of the NCSC and the AIVD can be found in respectively Appendices A.1.1 and A.1.2. The third system owner MIVD, has not been interviewed. Although the MIVD plays an important role in communication with military partners, their interests in the NDN are assumed to be largely aligned with those of the AIVD, as the agencies cooperate operationally in the NDN through the JSCU.

Perspectives on the scope of the National Detection Network are not aligned, as can be learned from the interviews. The perception of the National Detection Network of the system owners is a derivative of the organizations' missions. While the NCSC and AIVD share a responsibility for security of public organizations, their responsibilities diverge for private sector organizations. The NCSC has a legal mandate to protect cybersecurity of vital sector organizations[3], while the AIVD is responsible for *protecting the Dutch legal order through cybersecurity* in a broad sense[4] [A.1.2]. This is illustrated in Figure 4.3.

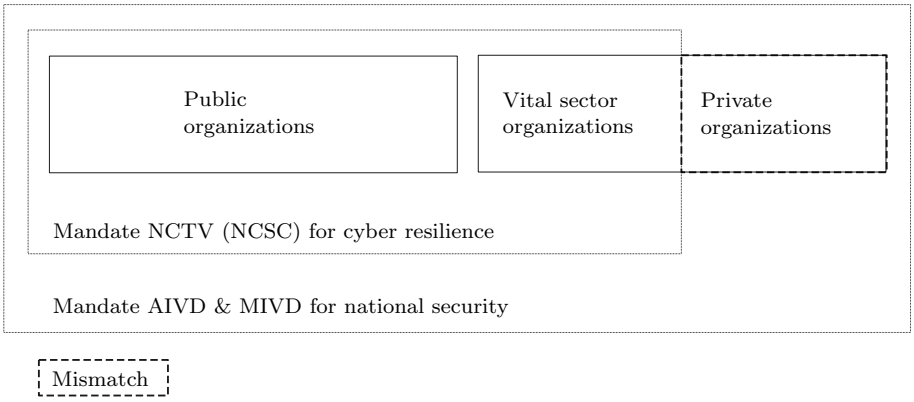

Figure 4.3: Diagram of the mandates of system owners NCSC [A.1.1] and AIVD [A.1.2]

The NCSC is responsible for management of the NDN technical systems described in Section 4.2, which is reflected in their perception of its goals. According to the NCSC, the aim of the NDN is to *contribute to resiliency of organizations in the Netherlands by exchanging threat intelligence* as well as *[help] these organizations build detection capability*, and *achieve situational awareness of cybersecurity threats* for both government and vital sector participants [A.1.1]. In this definition of goals, the NCSC focuses on the desired

[3]The responsibilities and mandate of the NCSC are codified in the Wet gegevensverwerking en meldplicht cybersecurity (Wgmc).

[4]As codified in the Wet op de inlichtingen- en veiligheidsdiensten (Wiv).

effects of sharing threat intelligence in a technical system.

The AIVD believes that the NDN is *a series of collaborations and should be seen as separate from the delivery mechanisms for CTI employed.* Furthermore, it states that *cooperation is not a goal in itself. The goal of the NDN should not be to exchange more threat intelligence, but rather to offer more suitable prospects for action ("handelingsperspectief") to targets of threats, for which the exchange of threat intelligence could be one of many means.* [A.1.2]. This definition by contrast perceives the NDN as a collaboration to achieve societal effects, independent of the means used.

Contrary to the AIVD's distinction between means and ends, most participants in the NDN [A.2] experience no such distinction between the technical systems they use and the NDN as a cooperation of organizations. For example, participants often refer to the NDN MISP system simply as 'the National Detection Network' [A.2.3, A.2.5, A.2.7].

While the AIVD shares indicators in the NDN that are derived from their research [A.1.2, Figure 4.2], it also shares information with NDN community members bilaterally [A.2.1, A.2.8], at least in part due to confidentiality requirements. This practice seems to be acceptable to the agency, and it states that *exchange of information could be done using the NDN infrastructure, via the NCSC, or in direct contact with a target. As intelligence service we could choose to bypass the NDN infrastructure and/or NCSC for reasons of need-to-know and source protection.* However, it later emphasizes that it would only use the current NDN systems for some indicators derived from their research, stating that *we will not share classified information in MISP, because MISP does not comply with our security standards for the exchange of classified information. We aim to use delivery mechanisms using the STIX/TAXII standards.*

This begs the question to what degree the AIVD is willing to commit to cooperation in the NDN on sharing unclassified threat intelligence. Possibly the current level of sharing only the indicators derived from confidential information is satisfactory, but likely more organizations would benefit from access to the information that is now being shared bilaterally. If the systems currently being managed by the NCSC do not meet security standards required for this, should a new delivery mechanism be developed (based on STIX/TAXII as proposed by the agency)? Could classified high-level intelligence possibly be structurally translated into unclassified indicators, suitable for sharing in the current systems? A clear vision on the role of the NCSC and the NDN community in achieving the AIVD's mission is not communicated in the interviews.

The system initiators are nonetheless important parties in the NDN, as they currently provide most value in the NDN by sharing information. Without agreement between these parties on the direction of the NDN it may prove hard to motivate participants to share information. Finding a working consensus between the NCSC and AIVD on the ambitions of the NDN may be seen as prerequisite solving other governance issues.

The prerogative of solving this stakeholder issue lies with the NCSC. As the NCSC has day-to-day ownership over the NDN systems, participants experience the NCSC as the 'owner' of the NDN. One participant described how *[t]he goals of the NDN are the same as the goals of the NCSC, the NDN is just one of their tools* [A.2.3]. The NCSC has internalized this, stating in response to a question about openness of the process that it *decides on the direction and tempo of the project, period* [A.1.1]. This is in line with the findings of Boeke (2018), who in a comparative review of national cybersecurity policy of four European countries, refers to the National Cyber Security Centre as being a central node for cooperation between Dutch government parties.

4.4 Findings

The National Cyber Security Centre has set up a community for sharing cybersecurity information: the National Detection Network. Currently 41 public and 21 private organizations are participating. Public organizations may place an IDS sensor in their internal network which automatically reports hits on the exchanged indicators to the NCSC, who use this information to enrich threat intelligence. Private organizations use the exchanged threat intelligence in their own detection infrastructure and can freely choose to report hits to the NCSC or not. This can happen either by analysts or in automated fashion.

From the interviews it can be determined that threat intelligence in the community is currently being shared primarily by the NCSC. Besides the sensors at public organizations reporting hits, not much information sharing takes place between parties in the NDN. Participants describe a lack of response from their peers and the NCSC when they incidentally did share information in the NDN.

A number of practical barriers to information sharing exist. The web-interface of the MISP platform is experienced as unfriendly, while organizations that have set up an automated connection with their own monitoring systems (and thus do not need the web-interface) report no such problems. Participants express their wish for support from the NCSC in automating the sharing process. On the other hand, one drinking water company wants to share more than is currently possible and finds itself limited by the NCSC definition of a 'sighting'.

However, practical barriers only account for some of the limited sharing behaviour. Organizations describe common goals of the National Detection Network and the ambition of community benefits brought by sharing information, but mostly do not act on this in practice. The discrepancy between individual and collective rationality is indicative of the existence of a collective action problem, as described in Section 2.3. Therefore not just practical barriers, but also stakeholder interests in the community are analyzed in this study.

The interests of participating organizations lie with protecting their primary business processes. The National Detection Network plays a role in this by helping improve their cybersecurity detection capabilities. Factors for the consumption of indicators in the NDN community are access to threat intelligence that has a low false-positive rate and is highly relevant to the organizations involved. The information in the NDN is considered to be of value due to its focus on the Netherlands, enrichment by analysts of the NCSC and intelligence agencies, and potentially through validation using sightings.

Factors for sharing of indicators and sightings in the NDN community are reported as: improved CTI data quality, economies of scale and financial advantages these bring, and collective security goals of the parties. However, even though organizations may formulate the added value of an active community this does not mean that they will engage in information sharing. Herein lies the collective action problem. This could be addressed through system governance, as described in Chapter 2.

As the NCSC maintains the NDN infrastructure, participants expect it to have an important role in governance of the community. The NCSC has internalized this role and determines system governance unilaterally. Some participants would like to become involved in decision-making about the NDN. A drinking water company even offers assistance in platform development. A prerequisite for successfully organizing governance for the NCSC lies in aligning its goals and role with those of the other system owners.

With these findings, the second sub-question of the study may be answered: *Are missing incentives limiting information sharing in the NDN?* The fact that participants refer to common goals, but mostly do not meet their ambitions to share is indeed indicative of the existence of a collective action problem that could be solved by introducing incentives. This forms the basis for the requirements and governance design in the following chapters.

However, the level of information sharing in the NDN community can not be attributed conclusively to the existence of a collective action problem, as some practical barriers to sharing information in the NDN community are also identified.

Chapter 5

Governance requirements for information sharing

Having established a knowledge base of cybersecurity threat intelligence sharing and collective action theory (Chapter 2), and taking into account the specifics of the case of the National Detection Network (Chapter 4), the design phase for improving information sharing in the system is now described.

The design consists of two elements, spread over this chapter and the next: high-level requirements for information sharing in cybersecurity communities (this chapter) and an instance of a design based on these requirements situated in the National Detection Network (Chapter 6). This relationship is displayed in Figure 3.1.

This chapter addresses the question: What are requirements of governance that improves information sharing? As this question is answered using both the details of the case and the knowledge base, this chapter is more conceptual than the next, which operationalizes these requirements using a process design specific to the case of the National Detection Network. As described in the next chapter, the requirements may be used to continuously assess the effects of the design in the system. Similarly, these requirements are used in the Discussion to verify that the proposed design is likely to achieve the desired information sharing.

The method used to generate a governance design in this study is that of Process Design (Bruijn, Heuvelhof, and 't veld 2010) as described in Chapter 3. In this method, governance measures based on these requirements cannot be seen separately, but influence each other in their effects in the system. The four elements of a good process design are openness,

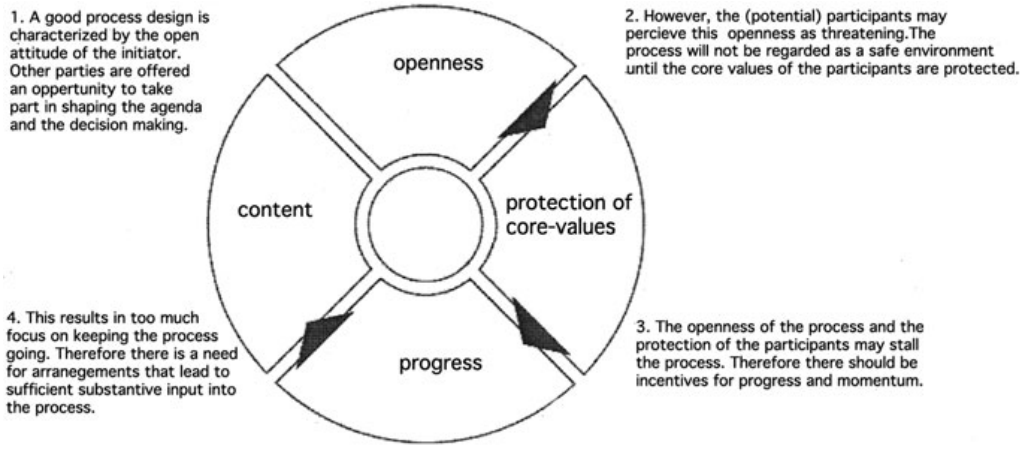

Figure 5.1: The four elements of a process design (Bruijn, Heuvelhof, and 't veld 2010)

protection of core values, progress, and substance, according to Bruijn, Heuvelhof, and 't veld (2010). These elements and how they relate are displayed in Figure 5.1. The requirements in this chapter are ordered by the respective process design element which they support. This structures the chapter, and provides insight into the relationships between the requirements.

The *MoSCoW* prioritization method is used to indicate the relative importance of each requirement on the overall goal to increase information sharing: from its formulation it can be seen if a requirement *must, should,* or *could* be used be used in the design.

5.1 Openness

Initiators of a cybersecurity community may want to determine norms and rules unilaterally. However, more openness in decision-making better suits a system in which parties are dependent on each other to achieve collective goals, like improved cybersecurity information sharing. This involves a change in perspective from individual to collective rationality, as described in Section 2.3. To make this change of perspective, the system initiators could consider how they for their own goals depend on outcomes of the community. As providing relevant information is central to the NCSC's mission, a level of active sharing in the NDN is highly relevant to this.

Requirement 1 *Must unite participants around a collective problem that is made explicit.*

Having the technological infrastructure to support sharing does not mean that it will happen. The basis of the community should be common interests between a group of organizations: collective action implies that there exists some shared problem. Starting from an existing group of well-aligned peers is the opposite approach of 'build it, they will come'.

This goal should be communicated well by the system initiators: this is why we share. This aids building trust in the community. As independent researcher Brown puts it: *you need a shared problem or experience to feel like you can trust someone with your sensitive information* [A.3.5].

Shared interests can exist either long-term due to mutual interdependence in a value chain or organizational alignment in a sector, or temporarily due to having shared experiences with a specific threat. An example of well-aligned interests is that of the regional cybersecurity community that is referred to in interview A.3.2. By cooperating regionally with organizations in the value chain, the high-tech company (who is not an NDN participant) is able to derive more relevant information sharing than it was in an ISAC. Shared interests could also be more high-level, like social or political goals.

Requirement 2 *Should have a clear legal framework for information sharing.*

Before engaging third parties, the system initiators should determine the desired scope of the system from their respective missions and mandates. Furthermore, they should consider the constraints put on information sharing by legal obligations. Relevant legal frameworks exist for example in data protection and freedom of information legislation. Communicating how compliance responsibilities are addressed by the system initiators may increase trust in the system.

In an interview with domain expert Geert Munnichs of Rathenau Institute, he states that there is a special role for government partners in cybersecurity communities: *they should not take a defensive stance in this discussion, but should actively plea for adequate oversight* [A.3.7]. Furthermore, Jaap-Henk Hoepman of the Radboud University argues that organizations participating in cybersecurity communities should be transparent about this to their customers [A.3.3].

5.2 Protection of core values

Although it is necessary for organizations participating in a community to have shared goals, in a process approach it should be recognized that in some instances they may also have diverging interests. The openness may therefore be experienced as a risk. System initiators should attempt to understand what drives participants in the community.

Requirement 3 *Decisions should be reached collaboratively.*

Those who are affected by a decision in the community should be allowed to influence it (Poteete, Janssen, and Ostrom 2010). In order to increase commitment to agreements made in the community, participants should be offered some way to collaborate on the decision so that they know that their core values will not be harmed by this. This increases commitment to the outcomes of a decision-making process (Bruijn, Heuvelhof, and 't veld 2010). For example: participant commitment to the agreed level of information sharing.

In the case of the National Detection Network, interests of participants are stated to be their primary business processes. Core values may however be broader, and include an organization's mission or worldview of its customers. Understanding these values well means that more promising proposals for sharing can be made.

Besides increasing commitment, collaborative decision-making may also result in reaching better substantive decisions, as more diverse views are involved in generating alternatives. Authors Shiffman and Gupta (2013) discuss these advantages of organizing cybersecurity communities 'bottom-up'.

Decision-making could be extended from the community to the development of infrastructure supporting it, i.e. the community should co-create its supporting infrastructure. In this way, the community can become a lead customer. If the cybersecurity community is supported by open source projects it can contribute to their development by supporting implementation of use cases specific to community needs. The NCSC supporting development of a sightings feature in MISP is an example of this [A.3.6].

5.3 Progress

Building on respecting core-values of participants is progress toward a collective action: improving information sharing in the community. Governance of cybersecurity communities must incentivize information sharing in order to prevent underinvestment. In this way, it can support realizing individual and collective benefits (Gordon, Loeb, and Lucyshyn 2003).

Requirement 4 *Must decrease the costs of sharing information.*

Consuming and sharing information is central to the idea of a cybersecurity community. Community governance must make it easier for participants in the community to share information. As domain expert Brown points out, sharing can be supported with a threat intelligence platform or something as easy as a Skype group [A.3.5]. If a cybersecurity community does not reduce costs of sharing (or disincentives otherwise), it will be of little benefit to its participants.

Sections 2.3 and 4.3.1 through 4.3.3 identify individual costs sharing cybersecurity information for the case of the NDN. Some participants in the NDN describe problems with automated sharing of indicators. Addressing such practical issues would quickly provide visible results for the NCSC.

In the long run, individual costs may be decreased by offering continuity or even assuring a level of service for a fixed period of time. Organizations may be more likely

to invest in their participation in the community, e.g. by integrating it in their security processes, if they can reliably calculate the return on this investment over time.

Requirement 5 *Should increase the individual rewards of sharing information.*

The positive network effects arising from cybersecurity communities are largely collective, i.e. not limited to those participants who committed to information sharing and paid the associated costs. As described in Section 2.3, this leads to a collective action problem.

Introducing individual rewards (or positive individual incentives) in the system may address this imbalance. A reward could be informal and simple as as recognizing a participant's efforts or providing event feedback. Establishing a social norm could be supported by reputational metrics that make the level of sharing of a participant explicit (Eeten and Bauer 2009; Eeten, Lone, et al. 2016).

More formal rewards could take the form of an exclusion mechanism so that positive network effects are individualized, effectively turning the public good into a club good (refer to Table 2.3).

Going beyond introducing individual rewards could involve introducing a regime of graduated sanctions for lack of sharing, leading up to an organization's exit from the community (Poteete, Janssen, and Ostrom 2010). Such graduated sanctions and rewards should again be determined through interactive decision-making. While imposing sharing demands or sanctions may seem strict, authors Fransen and Kerkdijk (2017) point to the example of ThreatAlliance: a cybersecurity community of vendors that requires of their participants to deliver 1000 malware samples per day (unique and not occurring in VirusTotal), simply in order to remain part of the community. While other communities do not need to match such high barriers to entry, the example shows how diverging levels of sharing can benefit different groups.

5.4 Substance

Progress towards improving information sharing and other aims of the community can also be too swift: it creates the risk of a decision-making process where some parties cannot keep up with progress. This risk increases as the number of participants grows and they become more diverse in terms of maturity and interests.

Requirement 6 *Large communities could be organized in nested enterprises.*

To address this, sub-configurations of participants or 'nested enterprises' (Poteete, Janssen, and Ostrom 2010) could be organized on differentiated levels that are more appropriate for their level of information sharing, effectively creating a new community for sharing cybersecurity information. The above requirements apply to the nested sub-configurations, meaning that they should again be formed around common interests. One could imagine temporary collaborations around specific threats in which a higher level of information sharing takes place. This could be facilitated by the same infrastructure as the original cybersecurity community.

Decision-making for the sub-configuration should be delegated: Requirement 3 applies and decisions should be influenced by those who are affected by them. The CiSP cybersecurity community of the United Kingdom uses sub-configurations of participants, who can decide for their group to be confidential (National Cyber Security Centre of the United Kingdom 2013). This is accepted by the respective system owner only if the request is motivated well, openness is the default.

Participants interacting in smaller groups promotes building trusted relationships within the community. As a rule of thumb, domain expert Brown indicates that twenty peers is

a suitable group size for sharing [A.3.5]. She points to the FS-ISAC as an example of how this happens in practice: although this organization has 4000 members, at its conferences natural sub-configurations form that collaborate naturally.

5.5 Overview

Requirements were proposed in this chapter that support the four elements of a successful process design according to Bruijn, Heuvelhof, and 't veld (2010). The requirements were based on the knowledge base of cybersecurity information sharing and the case description of the National Detection Network.

The third sub-question of the study can now be answered: *What are requirements of governance that improves information sharing?* Governance to improve information sharing in a cybersecurity community must unite participants around a collective problem that is made explicit. It should have a clear legal framework for information sharing. Decisions in the community should be reached collaboratively. It must decrease the costs, while increasing the individual rewards of sharing information. And it could organize large communities in nested enterprises.

Chapter 6

Improving information sharing in the NDN

Building on the requirements for improving information sharing, this chapter describes how the NCSC may shape governance in the National Detection Network community. This is the fourth sub-question of the study. The chapter describes a process in four phases for governance of the National Detection.

This design recognizes that there is no 'green field' at the outset: the National Detection Network is an existing community with an architecture and interests vested in it by the system owners and participants, as described in the case study of Chapter 4. The design is situated in this specific system at the time of writing, September 2018. However, lessons will be drawn for cybersecurity communities in general from the design in the Discussion chapter.

6.1 Overview

This chapter describes four phases by means of which new incentives for sharing threat intelligence and sightings by participants can be introduced in the current National Detection Network. To achieve this, collaborative processes and system architectures are shifted from 'one size fits most' to a differentiated nested approach. This is illustrated in the final phase of figure 6.1. This will allow the NDN to facilitate tight-knit sub-communities that increase trust among participants and create new incentives for engagement.

The four phases are based on the activities of the Process Design methodology of Bruijn, Heuvelhof, and 't veld (2010), as described in Section 3.2. The phases are illustrated in Figure 6.1. During the first phase, system owners NCSC, AIVD, and MIVD should reach consensus on the aims of the NDN, core concepts to their cooperation, and commit to a process approach. In the second phase, an initial attempt at interactive decision-making in the NDN community should be made in a small group of highly motivated participants. This group will function as a prototype for a 'trust circle' of a small number of participants that independently develops community norms. In the third phase, these norms should be converted to process agreements that would promote sharing for consecutive trust circles. This in preparation of the fourth phase, when an open process is started for NDN governance and participants in the NDN are free to enter into various trust circles in which the NCSC is mostly a facilitating partner.

This chapter goes into the four process design phases in order. In the final section, intermediate conclusions are drawn from the case of the NDN.

Before starting, a word about the distinction between 'process' and 'substance' throughout the chapter. This design describes how communities can determine what norms are suitable in their context for improving cybersecurity through information sharing. It does

this by separating substance (e.g.'what constitutes a sighting?') from process ('how to decide what constitutes a sighting?').

Although a system owner needs to be flexible when engaging in an interactive decision-making process, they are free to pursue their interests in shaping the process. The goal of the NCSC is for the NDN to become a more active community, and therefore it should attempt to steer the process in the direction of substantive choices that support this goal. This can be seen as leadership in the process. When opportunities to pursue substantive choices in support of the NCSC's goals arise, they will be highlighted as such in the text. It is however important to note that the process can be successful even if it takes a different direction from the original goals of the system owners. The leadership recommendations should therefore be seen as substantive suggestions op top of the process approach.

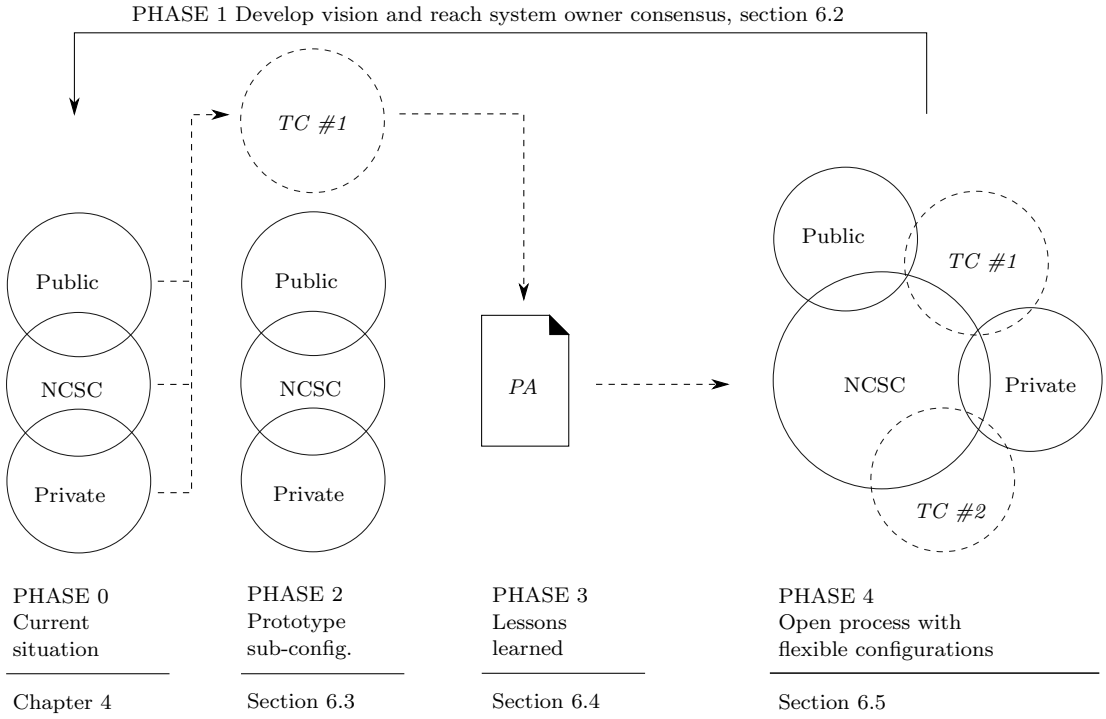

Figure 6.1: Four phases of the process design, with corresponding chapters

6.2 Reach system owner consensus

A clear vision on future of the National Detection Network community is needed to start a process that works towards improved collaboration. While a level of ambiguity can be acceptable or in some cases even productive (as will be discussed) the system owners NCSC, AIVD, and MIVD need to address three issues on their cooperation before engaging parties in the second phase.

6.2.1 Resolve system owners' mandates

There exists a mismatch in missions and mandates of the NCSC on the one hand and intelligence agencies AIVD and MIVD on the other hand. As discussed in Section 4.3.3,

the agencies are responsible for cybersecurity in a broad sense, while the NCSC has a legal mandate to focus on public and vital sector organizations only.

As long as the NDN allows only vital sector private organizations to participate, this will therefore make achieving commitment to the process difficult: the agencies will continue to have a need to share information outside of the system, thus undermining the network effects of the NDN.

The effects of sharing outside of the NDN can be seen in practice in interview A.2.1, where a strategic security expert of a bank described: *The added value of the NDN lies in receiving information that we cannot get from other sources. The first is CTI from intelligence agencies. In the past we've also been asked to exchange CTI with the agencies outside of the NDN, which made this added value less clear.* Other interviews echoed the involvement of the agencies as reason for their engagement.

Process activity 1 *Reaffirm shared goals of the system owners, from which system scope and participant entry criteria should follow.*

These criteria could be based on the role of the organizations in Dutch society or their possible contributions to the community. Organizations not currently considered 'vital sector' can be valuable targets. Take for example the AEX-traded high-tech company of interview A.3.2 that might both have important social and economic value and be able to make valuable contributions to the NDN community, but is currently excluded from the NDN constituency as it is not considered vital sector. Another example might be healthcare organizations like hospitals, which are not considered to be vital sector but clearly fulfill a relevant social function. If current legal frameworks (see Figure 4.3) are unnecessarily limiting the constituency of the system, these frameworks or their application should be changed.

It is not necessary to formulate a conclusive list of entry criteria, and decisions on entry can be later made on a case-by-case basis. The reason for conducting the activity is primarily to align interests between the system owners.

Leadership opportunity 1 *Expand NDN community in the short term by including relevant (sectoral) CERTs as intermediaries.*

To start the process in the short term, it might be possible to work around institutional limitations which prescribe a vital sector constituency. The NCSC is mandated to provide services to CERTs, and could use this to involve non-vital but relevant organizations through their CERT. For example, by including the healthcare-focused Z-CERT, or the regional CERT of the high-tech company described in interview A.3.2. The exchange of threat intelligence with the sectoral CERTs, or between the sectoral CERTs and their constituent organizations, could well be facilitated by the existing NDN infrastructure.

6.2.2 Define core concepts

As described in Chapter 2 the field of cybersecurity knowledge sharing is very much in flux, and concepts are still being established in practice. There is no commonly accepted definition of threat intelligence or a threat intelligence platform. System owners should nonetheless attempt reach consensus on their interpretation of a small number of core concepts, as this is necessary to communicate expectations to the participants.

Concepts chosen should relate to the desired results of the NDN, and not the means used to achieved them (i.e. the technological systems). Concepts to define include:

1. High-level threat intelligence (TTPs), and suitable taxonomies;

2. Low-level threat intelligence (IoCs), and suitable taxonomies;

3. Sightings; and

4. Situational awareness.

Concepts can be derived from current practice and the desired outputs of the NDN. The emphasis here is on the system owners establishing *their* interpretation: a working definition that may be refined during the process is sufficient at this stage. This activity again serves the purpose of aligning perspectives of the system owners.

This exercise serves to go beyond the obvious and be forced to create a working definition that could later form the basis of technical specifications. Such specifications are necessary when asking outside parties to extend their information systems to the NDN community. For example, contrary to the MISP definition of a 'sighting', participants in the NDN want to share more information than is currently possible, like negative sightings [A.2.3, A.2.5, A.2.7].

The MISP API is a form of a de-facto specification. However, for its information exchange the NDN should not be guided by existing solutions, but rather by the system owners' vision of core concepts, later refined with the community.

Process activity 2 *Establish concepts central to the system. Define what is meant in context of the NDN by terms like TTPs, IoCs, sightings, and situational awareness.*

A tolerance for ambiguity serves a purpose in the process: stakeholders can become divided over concepts that have been too narrowly defined. Therefore only core concepts should be defined. Additionally, not discussing unnecessary definitions speeds up progress. During the process, working definitions can be refined if necessary.

Process activity 3 *Define system security assurance level, using a technical standard or third party assurance (i.e. an auditor or the AIVD).*

One especially relevant concept to define before starting the process is 'security'. What threats should information shared in the NDN be protected against? What are considered unacceptable risks? Making clear agreements will serve the system owners in the long term, as this promotes trust when participants start sharing their intelligence on NDN systems. Another advantage is that if a security level is defined, the responsibility of the system owners becomes bounded.

6.2.3 Establish that a process approach is necessary

Collaboration in cybersecurity communities like the National Detection Network is an example of an unstructured problem: no authoritative solution exists for it. This is because the problem to be solved is uncertain (i.e. what entails collaboration for cybersecurity detection) and solutions are still dynamic (e.g. standards and practice of capabilities). Additionally, there is no consensus about the criteria for solving the problem yet (Bruijn, Heuvelhof, and 't veld 2010).

In this sense, the National Detection Network is a cutting edge collaboration and an interesting prototype for other cybersecurity communities. As a result, a purely substantive approach to decision-making will be of limited value, as there exist no conclusive answers. Therefore some degree of interactive decision-making or negotiation with participants will be necessary. This may be structured using the process approach that is the methodology used in the thesis research.

Process activity 4 *Gain system owner commitment for starting an interactive decision-making process.*

The cooperation between NCSC, AIVD, and MIVD in the National Detection Network cooperation has existed since 2012 and has over the last year become more productive [A.1.1]. The parties should have reached a decision if they share a common responsibility and mandate for cybersecurity in the Netherlands through the activities described in Section 6.2.1 and if they share some vision of the solutions through determining concepts. This shared understanding of a problem is the primary condition for engaging in a process.

The second condition for parties to enter into a process is for there to exist a sense of urgency between them to solve their problem together. Parties must only engage in a process if they are convinced that it is the best way to address their common problem, according to Bruijn, Heuvelhof, and 't veld (2010). The decision for the NDN system owners is therefore if they can and want to commit to the process approach: either to the governance design as described in this chapter or a variant thereof.

If parties engage in a process without a sufficiently high sense of urgency this forms a risk, as they may not be willing to commit to the outcomes. The possibility of this happening in the NDN becomes apparent when the AIVD describes how it reserves the right to *to bypass the NDN infrastructure and/or NCSC* [A.1.2]. This is an indication that they have an alternative to cooperation with the NCSC, and may be unlikely to make concessions or work towards shared solutions. Commitment may still be achieved by offering a prospect of a valuable enough outcome for the AIVD, for example situational awareness achieved from an NDN community that shares sightings.

Parties are better off not to engage in a process for which system owners are not able to establish a shared problem definition, or no high sense of urgency to engage in a process of interactive decision-making exists. An alternative form of cooperation can be envisioned in which the NCSC manages the NDN infrastructure like in the current situation, but the intelligence agencies become participants in the community and share opportunistically. However, strong involvement of the agencies also motivates participant engagement as described in Section 4.3.3.

6.3 Engage motivated participants in trust circle

In order to increase trust, large communities should be broken down into smaller configurations, as independent expert Sarah Brown proposes. As a rule of thumb, she lists a maximum of twenty organizations. [A.3.5].

In the second phase, the NCSC should begin interactive decision-making at small scale. A group of already motivated participants of the NDN should be proposed to start cooperating in a sub-configuration of the NDN community, which will be referred to as a 'trust circle' throughout the thesis. The group should be given access to the NDN sharing infrastructure and given decision-power over their sharing norms. This could happen within the existing NDN infrastructure by leveraging MISP *sharing groups*. Alternatively, dedicated MISP instances could be set up for each trust circle in the community, or some other platform could be used.

This initial trust circle will function as a prototype that may support development of process agreements for future such trust circles that the NDN will facilitate. The idea of establishing trust circles was proposed by an employee of the NCSC [A.1.1].

The parties for the initial trust circle are chosen through an actor scan. This section gives suggestions on how to draw them into the interactive decision-making process and how to manage expectations.

6.3.1 Actor scan

Based on the interviews of Chapter 4, the participants can be mapped to one of four categories, determining the strategy the NCSC should use to engage them in the NDN network. This stakeholder analysis is based on the 'power vs. interest' grid. For the context of cybersecurity communities, power is redefined as CTI capability level (Kerkdijk and Koens 2017) or the 'power' to deliver valuable intelligence, and interest is redefined as the level of sharing and engagement in the community.

Process activity 5 *Determine CTI capability and community engagement levels for (potential) participants.*

The results of the actor analysis are displayed in Figure 6.2. Note that not only current participants, but also the high tech company of interview A.3.2 is listed. The system owners should perform an actor analysis for current and potential participants which they determined to be in the NDN scope through the activities described in Section 4.3. Interviews or questionnaires could be used to place potential participants in one of the quadrants of Figure 6.2.

In the current phase, only organizations should be involved in interactive decision-making that are both mature and active, i.e. that are located in the top-right quadrant of Figure 6.2. From the interviews this would be Bank #1 and Rijkswaterstaat. Rewarding these organizations for their engagement with the NDN creates the beginnings of a social norm in the community. Strategies for addressing organizations in other quadrants will be discussed in the next section. No resources should be spent on involving organizations in the bottom-left quadrant.

Process activity 6 *Fit communication to point of contact role responsibilities and organizational maturity level.*

From the organizations in the 'reward' quadrant, many possible trust circles will likely be diverse in terms of sector and type of organization. This need not form a barrier to cooperation between these parties, and in fact cross-sectoral intelligence sharing will even result in enriched awareness. However, when involving diverse organizations the tone and expectations of communication must be carefully matched to the point of contact's role and their organizational maturity level.

A word about language and framing. When communicating about the cooperation, the NCSC should from this phase onward no longer speak of 'products' which they offer to their 'constituency', as this promotes a passive stance from participants. Instead the NCSC should speak in more collaborative terms, like 'co-creation of infrastructure' or 'interactive decision-making for the network'. This promotes an active role for participants in the process.

6.3.2 Stimulate early participation

Parties should be motivated to enter the process. This may be done by showing swift progress on substantive decision-making toward information sharing.

Process activity 7 *Start initial trust circle by offering participants in the 'reward' quadrant of the actor analysis quick-wins.*

As discussed in Section 4.3.3, parties have described their wish to share more than is currently possible. For example by reporting back non-sightings, i.e. when an indicator was not found on their network. Such proposals could be on the agenda for interactive

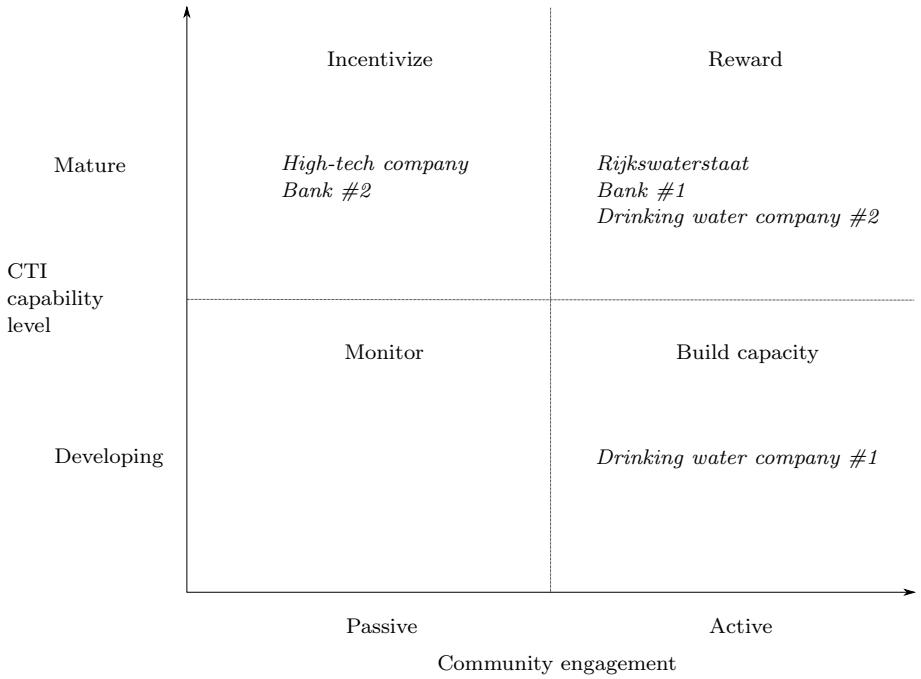

Figure 6.2: Actor analysis of CTI capability vs. engagement in NDN community

decision-making in the initial trust circle. This provides the participants with the prospect of quick-wins toward seeing their interests met. Using active participants as ambassadors becomes possible too, e.g. by having parties who have automated their sharing process share their experiences. This may form the basis of an initial voluntary plan of action for the NDN community participants.

Leadership opportunity 2 *Set up an action plan for all motivated participants in the NDN, which includes committing to automation and collaboratively establishing definitions of e.g. sightings.*

Although all organizations in the NDN might benefit from quick-wins and exchanging thoughts with active participants, it is critical that quick-wins are offered to the most active participants in the initial trust circle first. In this way, the parties are rewarded for their engagement, and their exchange will reinforce this engagement. Progress might slow down if more parties are added at this stage.

6.3.3 Provide system expectations

While decisions on interactions in the NDN should be formed using an interactive decision-making process, there are outer bounds of what the NCSC can offer in terms of managing the infrastructure. These outer bounds are formed by legal restrictions (like FOIA and data protection legislation) and should be well-defined and communicated by the system owners.

Even if restricting their design space, participants will likely welcome information on outer bounds of the cooperation. System continuity enables participants to do investments in the cooperation, e.g. in automating their connection to the NDN, because they can better calculate their return on investment under predictable conditions.

Process activity 8 *Communicate system outer boundaries and vision. Communicating clear expectations is a precondition to achieving participant commitment.*

Defining and communicating a full system development roadmap may not be feasible at this point. Alternatively, the system owners can create an interface through which participants access the NDN infrastructures, and guarantee upward compatibility on it: when new features or concepts are defined, the interface would remain functional for the participants. The complexity of the systems would then be abstracted behind the interface, so that the community can rely on it, while still offering flexibility to the NCSC for development of the systems. The interface could be the MISP API, however this currently does not assure any type of upward compatibility, nor is its development controlled by the NCSC.

Leadership opportunity 3 *Address ambiguity between MISP and TIP systems. Provide NDN roadmap or assure upward compatibility on a participant API.*

6.4 Formulate process agreements

In the third phase, lessons should be drawn from collaboration in the initial trust circle. These lessons can be cultivated as social norms or formalized as rules. Establishing norms or rules serves the function of establishing trust, as well as countering free-rider behaviour (Ostrom 1990). These could be social norms or formal codified norms.

This section describes dilemmas that should be addressed by the process agreements. These agreements can be used to structure interactions in the initial trust circle, but also be used as a blueprint for the consecutive trust circles of phase 4 in which participants might be otherwise less inclined to share.

Formalized process agreements may take the form: *'Parties will ...'*. When deciding on process agreements, parties should work from substantive variety to selection, i.e. start wide and end focused (Bruijn, Heuvelhof, and 't veld 2010). While discussing a diverse selection of topics may build trust, parties should resist the temptation to codify all aspects of their cooperation as this reduces flexibility: establishing informal social norms may be as effective.

Process activity 9 *Collaboratively formulate process agreements based on lessons learned in initial trust circle, in the form of social norms to establish or rules to formalize.*

Although process agreements are the result of an interactive decision-making process, the NCSC can do substantive proposals and steer the collaboration in a desired direction. The introduction of reputational norms that promote desirable information sharing behaviour should be proposed for the process agreements.

These proposals are aimed at the organizations in the top-left and bottom-right quadrants of Figure 6.2, nudging them to move to the top-right corner of organizations where organizations are both mature in their CTI capability and engaged in the NDN process.

Process activity 10 *Introduce comparative reputational metrics to incentivize and reward engagement. Highlight leaders in the community to establish a norm of sharing.*

In order to achieve collective action through sharing of sightings, the 'carrot' approach should be attempted before the 'stick'. Information sharing can be made explicit using reputational metrics (Eeten and Bauer 2009; Eeten, Lone, et al. 2016).

Metrics could include for example: the number of contributions to the community in terms of (unique) events, responses to events shared by other participants, or (negative) sightings reported. These numbers could be normalized by the number of analysts in an organization's SOC. Some understanding of the types of threat intelligence exchanged could also be used for rewarding organizations when they share valuable information.

Importantly, metrics must measure the level of information sharing and *not* organizational or technological maturity. It is important to design the metrics so that they do not create perverse incentives. For example, metrics should not measure the number of incidents reported, as this incentivizes insecurity (Gordon, Loeb, and Lucyshyn 2003). Similarly, metrics that measure sharing should not be a proxy for capability level, as this does not offer equal opportunity to smaller organizations.

Leadership opportunity 4 *Use the process to raise maturity through participant mentoring and NCSC knowledge-sharing at regular meetings.*

In a cybersecurity community like the NDN, both threat intelligence and other types of knowledge may be shared. For example, experiences with setting up capabilities, and lessons learned from other collaborations. While capacity building is not the focus of this study, it may support the goal of increasing information sharing by increasing the group of of participants with mature detection capabilities. To this end, the NCSC could provide opportunities for organizations to learn from one another by organizing regular meetings. Once again, roles in the respective organizations should be matched so that lessons apply to the persons meeting.

To promote knowledge sharing, the NCSC could communicate its existing factsheets (e.g. on how to set up a SOC) at regular intervals to aid participants developing their capabilities. In addition, it could explore endorsing certain providers of solutions or SOC-as-a-service without thereby creating government market disruption.

The rest of this section describes some of the dilemmas the NCSC and participants may face when formulating process agreements, as suggested by Bruijn, Heuvelhof, and 't veld (2010), namely: entry and exit rules, confidentiality agreements, and the decision-making mechanism itself. These issues will have to again be addressed collaboratively in the community.

6.4.1 Many or few parties

Group size of a trust circle should be determined by the context, and therefore parties in the respective group can best determine who can enter. Criteria could for example be formulated based on organizations being active in some sector, having certain capabilities, or having experience with a specific threat.

A community sub-configuration like a trust circle could arise naturally out of a shared goals, or vice versa a group of cooperating parties could formulate a goal for their cooperation. A diverse set of circles can arise if ISACs and ad-hoc circles are facilitated, as displayed in Figure 6.1.

An attitude that would not be productive in an interactive decision-making process is how the NCSC employee described current entry rules for the NDN: *New participants are able to enter the project if we agree that it would be relevant.* [A.1.1]. Rather, entry rules for trust circles as well as the NDN community as a whole should be determined collaboratively.

Making exit rules delineates a trust circle by describing how parties can end their cooperation. This also promotes an active role, as exit rules make explicit what happens when a party does not fulfill its responsibilities, e.g. in terms of sharing or confidentiality. Where rewarding organizations using reputational metrics forms the 'carrot' (in Process activity 10) the exit rules form the 'stick'.

6.4.2 Public or confidential

Parties in a trust circle must decide on the public nature of their cooperation, both in terms of process and substance. Process agreements may serve building trust on both

types.

Leadership opportunity 5 *Allow participants to determine their own confidentiality and security requirements, within bounds set by the system owners.*

Confidentiality in terms of process relates to who are cooperating and to what ends. Many CTI communities are public in their existence, for example the European Government CERTs (EGC) group shares the names of its members on its website. However, there may be good reason to keep the names of participants in a trust circle in the NDN confidential. The names of organizations in an ISAC should for example not be public, in order to not reveal what organizations are considered 'vital', and membership of an ad-hoc group formed around a certain threat might remain confidential in order to not reveal information about what threats participants are faced with.

Confidentiality in terms of substance relates to what knowledge is shared and who is impacted by a certain threat. In other words, the data that is being shared in the cybersecurity community. Transmission principles can be made explicit through agreements about using the Traffic Light Protocol for secondary sharing, as described in Section 2.2.2. Or through first or third party assurance about security level of systems where shared information is processed at the participants. Imagine for example a certification scheme for handling of sensitive or classified information.

Depending on the organizations in the trust circle, participants may or may not want for events or sightings to be related back to them; as this might pose a security or reputational risk. The more control participants themselves have over transmission principles when sharing, the more likely they are to share information.

However, confidentiality agreements that are too strict could also pose a barrier to entry to a trust community. Meeting high security norms or changing organizational processes may not be feasible for participants who still developing their capabilities. This is another reason to let circles determine their own confidentiality agreements. However, minimum requirements of system security and confidentiality when sharing may be set by the system owners.

Leadership opportunity 6 *Explore privacy enhancing techniques for e.g. obfuscation of event source or hit context. Facilitate anonymous contact channel.*

The NCSC might propose features in the roadmap of NDN infrastructure to optionally anonymize contributions, thus reducing the risk for participants when sharing. Such privacy-preserving trust mechanisms are described in Section 2.2.2, possibly ranging from simple aggregation to sophisticated secure multi-party computation. Likely such measures would pose performance limitations of the system, therefore interactive decision-making becomes relevant to make these trade-offs. Additionally, the NCSC could facilitate a contact channel for parties who wish to share knowledge bilaterally without revealing their identities.

6.4.3 Quick results or accurate decisions

Finally, the procedure for reaching decisions itself should be arranged. In working through the above dilemmas, participants in a circle should have gained initial experience with interactive decision-making.

Parties should then decide if they need formal structures like a chairmanship or regular meetings to come to further agreements. Formalizing decision-making is a trade-off, where parties may prefer to achieve quick results or have the opportunity to reach consensus (speed vs. core-values). A structured decision-making process promotes commitment to

a planning or budget that participants can develop for their trust circle, for example in order to meet confidentiality to establish norms.

Finally, participants should determine if there is a desired end state after which their cooperation would be no longer necessary, for example after successfully analyzing a threat in an ad-hoc circle.

6.5 Networked governance

In the fourth and final phase, the interactive decision-making process leaves the prototype stage and all members of the NDN community are able to enter into trust circles. Members can be a part of various configurations, for example sharing threats relevant to their sector in one circle, and analyzing a specific group of events in another. The NCSC can be seen as a facilitating partner in each trust circle, as it provides the infrastructure used for sharing and therefore gets access to the exchanged intelligence.

Process activity 11 *Continuously apply learned lessons to support the creation of new trust circles.*

Process agreements from the third phase may be used as 'template' to start new circles with minimal effort. Considering that template process agreements are derived from the initial circle with highly engaged members, using its process agreements can have the effect of promoting information sharing in consecutive circles as well. However, circles should be able to decide among themselves on which social norms and formalized rules they choose to adopt. A varied set of circles may arise in terms of means and ends of collaboration.

The role of the NCSC remains to share valuable information with participants, only with the added possibility of sharing certain information with specific circles within the NDN community.

Process activity 12 *Continuously evaluate if the system meets its goals.*

Finally, the system owners together must manage the overall direction of the National Detection Network. To monitor this, they can use a the requirements for information sharing as described in Chapter 5, as well as the scope determined through Process activity 1. Individual interactions in the various trust circles will have become more diverse through introduction of trust circles with diverging rules. The challenge is to manage the circles at micro-level in order to achieve the desired effects at macro-level.

6.6 Design conclusions

This chapter described a design for governance that promotes information sharing in the National Detection Network. The fourth sub-question of the thesis may now be answered: *How can the NCSC shape governance in the NDN community?* In an process consisting of four phases, the NDN community can move toward a structure of trust circles for improved sharing information.

Decisions in the proposed governance are reached collaboratively with participants through interactive decision-making, starting out in a prototype of a 'trust circle' with a small number of highly engaged participants. Lessons learned from this prototype are then used to set up further such sub-configurations in the community.

The design describes phases in the process, activities that should be carried out, and dilemmas that system owners will faced with in their governance of the system. Opportunities for leadership are presented to steer the community in a direction that is consistent with the aims of the system owners. However, adopting interactive decision-making means

that the system owners will occasionally see the interests of other parties in the NDN prevail.

This design is proposed while the field of cybersecurity information sharing is in constant development. Similarly, the community of interest is rapidly growing and changing. Recommendations specific to the system may therefore be soon outdated. However, lessons from the process design will be drawn in the next chapter.

Chapter 7

Discussion

Findings from the previous chapters are reiterated here before answering the main research question. Possible bias and limitations of the study are considered and alternative approaches are discussed. By means of verification and validation of the case and the design assumptions, it is then determined if the findings could be generalized to cybersecurity communities in general.

7.1 Findings

The first sub-question of the study is: *What factors determine the level of information sharing in a cybersecurity community? (Section 2.4)* While an organization's consumption and analysis of of threat intelligence is mostly determined by its detection capability levels, its level of information sharing is determined by the individual costs and collective benefits associated with sharing in the community.

This can be understood from the perspective of collective action theory: organizations consume information as this benefits their individual detection capabilities, but because the rewards for sharing information in a cybersecurity community are collective rather than individual, incentives to share information are often missing in cybersecurity communities.

Is this the case for the National Detection Network? The second question is: *Are missing incentives limiting information sharing in the NDN? (Section 4.4)* Through an analysis of the case of the National Detection Network of the Netherlands and 19 interviews with domain experts and participants this question is answered.

The continuity of primary business processes is the main interest of participants in this cybersecurity community. The NDN provides them with access to cybersecurity information that is seen by the participants as relevant and validated by the intelligence agencies of the Netherlands. Factors that motivate participants to share threat intelligence in the NDN community are economies of scale, improved data quality, and achieving common security goals.

Although these are collective goals, participants mostly do not meet their information sharing ambitions. This found to be indicative of the existence of a collective action problem that could be solved by introducing incentives. However, the level of information sharing in the NDN community can not be attributed conclusively to the existence of a collective action problem, as some practical barriers to sharing information in the NDN community are also identified. Design principles from collective action theory are nonetheless seen as promising, and therefore explored.

This foundation of a knowledge base and case description with interviews was then used to propose a design in two parts: requirements of information sharing in cybersecurity communities, and a governance design for the case of the National Detection Network. The method used is described in Chapter ch:method.

The third question begins the design cycle: *What are requirements of governance that improves information sharing? (Section 5.5)* Governance to improve information sharing in a cybersecurity community must unite participants around a collective problem that is made explicit. It should have a clear legal framework for information sharing. Decisions in the community should be reached collaboratively. It must decrease the costs associated with sharing information, while increasing the individual rewards. And finally, it could organize large communities in nested enterprises. The requirements are formulated using 'must, should, or could' to indicate a prioritization. The requirements support the four elements of good process design: openness, protection of core values, progress, and substance (Bruijn, Heuvelhof, and 't veld 2010).

The fourth sub-question of the thesis is: *How can the NCSC introduce these measures in the NDN? (Section 6.6)* A governance design is proposed consisting of four phases, through which the NDN community can move toward a decentralized structure using 'trust circles' that are facilitated by the existing sharing infrastructure. Trust circles are nested sub-configurations of the NDN community that promote trust. Comparative reputational metrics are introduced in order to make the level of sharing of each organization explicit.

In the proposed governance structure, decisions are reached collaboratively with participants. The process starts out with a single trust circle with a small number of highly engaged participants. Lessons learned from this prototype are then used to set up further such sub-configurations in the community, in which participants may collaborate with peers who are similar to them in terms of maturity or sharing ambitions. Trust circles may exist indefinitely in the NDN, for example for cooperation in a business sector, or come about ad-hoc for cooperation between organizations that are faced with a certain threat, and be terminated when goals have been reached.

The design describes dilemmas that system owners will be faced with in their governance of the system, and distinguishes between process activities that should be carried out for interactive decision-making, and opportunities for leadership in this process for the system owners. However, adopting interactive decision-making means that the system owners will occasionally see the interests of other parties in the NDN prevail. Accepting this might well lead to a higher level of commitment from participants.

The main research question can now be answered: **How can information sharing in the National Detection Network be incentivized?** The NCSC can make collective goals of the NDN community explicit by involving participants in a process of interactive decision-making, where peers are motivated to share information in decentralized trust circles by instituting comparative reputational metrics.

7.2 Research bias and limitations

This section considers the outcomes of the study in light of possible shortfalls of the chosen method. Especially unexpected results point towards such limitations and are therefore discussed.

7.2.1 Lens of collective action

Looking at the field of cybersecurity knowledge sharing using methods from the social sciences may yield valuable new perspectives on problems, as is argued in this study. However, the law of the instrument applies: to someone with a hammer, everything looks like a nail.

The risk is that the problem studied is made to fit the mold for a solution. This question goes back to epistemology and is arguably not something that will be solved in this study, but its influence can be reduced by considering multiple perspectives or approaches for a

problem (Allison and Pomeroy 2000). In a way, using theory from the social sciences to look at a technological system already is an example of combining different perspectives to a problem. But the approach is nonetheless liable to the same fixation on solutions in a certain direction, in this case that of collective action design.

This study has attempted to assess critically if the method of collective action actually theory applies to the problem of cybersecurity threat intelligence sharing in Sections 2.3.3 and 4.4. It cannot be established that sharing cybersecurity information leads to the creation of a pure common-pool resource, which is the starting point of the Ostrom (1990) for designing for collective action. This is because not only can threat intelligence be used without preventing others from using it (i.e. the good is non-rivalrous), the opposite may in fact be true; where the network effects increase as information is shared more widely.

However, as discussed in Section 2.3 there is some form of collective action as described by Olson (1965) necessary for cybersecurity information sharing because of the free-rider problem first established by Gordon, Loeb, and Lucyshyn (2003).

Intuitively there is therefore reason to explore the domain of collective action design. This intuition is reinforced by statements from the interviews in which participants in the community speak about collective goals, such as their common security interests and enriching threat intelligence as their motivation to share. This is further described in Section 4.3.3.

Authors Shiffman and Gupta (2013) reflect on cybersecurity while taking lessons from 'the commons' in a broad sense, thereby avoiding specific definitions of the goals which a community might have. Although applying to a broader field than threat intelligence, the authors draw similar conclusions on the potential usefulness of collective action theory for the problem of cybersecurity information sharing.

7.2.2 Cultural policy bias toward interactive decision-making

National cybersecurity policies of four European countries are compared by Boeke (2018), who finds the policy of the Netherlands is characterized by "trust and equality". He describes the institutional context of cybersecurity in Dutch government as "a participant-governed network".

The choice for the case of National Detection Network, situated in the policy context of the Netherlands, may have resulted in a bias toward solutions driven by this trust and equality. Perhaps not coincidentally, the name of the cybersecurity community of interest includes the word 'network'.

While the collaborative approach using interactive decision-making is therefore fitting for the case of the NDN, a collaborative approach is not necessarily always better. An alternative approach to the design proposed in this study may be seen by looking at how the government of the United Kingdom takes a more unilateral approach and prescribes terms and conditions for organizations wanting to participate in its CiSP cybersecurity community. Currently some 4000 organizations are participating (National Cyber Security Centre of the United Kingdom 2013).

The choice for an collaborative versus unilateral approach depends on the context of the community and organizational culture of the involved organizations. That is to say, using the terms and conditions of the CiSP for other communities like the National Detection Network may not lead to similar results.

7.2.3 Perspective of national regulator

In the case of the National Detection Network, the community was initiated by the national government, specifically the National Cyber Security Centre. It is responsible for

protection of vital sector organizations, and these are often organized on a national level: the goals of the NDN are aligned with the NCSC's broader mission. Nonetheless, the perspective and scope of the case study and corresponding design should be critically assessed, as this influences if requirements derived from the case research could apply to cybersecurity communities in a broad sense.

Furthermore, the problem of cybersecurity threat detection is not necessarily best served by a national scope. It also can be argued that the European regulatory level is more suitable for information sharing on cybersecurity threats, as parties are more diverse and economies of scale are potentially greater. Authors Settanni et al. (2017) propose an incident sharing system for collaborative analysis between European CERTs. Although the European Union has no legal competency on issues related to national security, a body like ENISA could coordinate voluntary cooperation between CERTs or private organizations residing in Member States.

Similarly, a regional cooperation between high tech companies may form a substitute for participation in the National Detection Network as described in interview A.3.2. Cybersecurity communities need in fact not be tied to a public body at all. Any organization willing to coordinate interactions between parties to improve sharing of cybersecurity information could achieve these same goals. Arguably, multinational technology companies have more experience and means to direct toward the same goals as national regulators and may therefore be as suitable to organize a cybersecurity community. What's more, technology companies and governments share a common interest in secure and reliable networks.

7.2.4 Interview selection

An unexpected result was to find that the interviewees were aware of risks to their respective organizations of participating in the NDN, e.g. in terms of compliance or reputation, but considered these to be outside their influence, so that colleagues in their organization would need to deal with them (i.e. legal or risk departments). Two questions of validity arise in explaining this finding.

First, there exists the risk of selection of more engaged participating organizations. This is in part because the NCSC helped facilitate the interviews, and it is likely to have good relations with more engaged participants. A less important factor may be self-selection by the interviewees: all participants requested to conduct an interview with responded positively as discussed in Section 3.1.1.

The second question of validity is that of selection of interview subjects with more engaged roles within those organizations. The chosen method attempted to increase validity through speaking to people in two roles: one in an operational role, one in a strategic role. However, all interviewees were involved with or strategically responsible for security operations, and saw the benefit of exchanging threat intelligence. Their perspectives within organizations could have been tested by also speaking to persons in legal or risk roles.

7.3 Case generalization

The degree to which case-based research can be used to make general statements is influenced by limitations of the study. As discussed above, there may exist a bias towards governance solutions in the social science perspective. Furthermore, the case study has the national government perspective, which is involved with and committed to this system, and is arguably also inclined to think in terms of governance solutions. Finally there is the risk that the interviewed participants were not representative of the population in terms of their engagement in the community.

With these limitations in the approach in mind, it will now be assessed if the results can be verified and validated.

7.3.1 Verification

Because the design cycle of this study describes the requirements for improving information sharing (Chapter 5), it can be determined if the proposed governance design (Chapter 6) meets these requirements. In other words: did the author make what he said he would make?

Chapter 5 describes how the requirements contribute to the four elements of good process design according to Bruijn, Heuvelhof, and 't veld (2010), which are openness, protection of core values, progress, and substance. The design then lists the process activities that make up the four phases by which the NDN could move to the new governance model. Process activities of the design are mapped to the requirements for improved information sharing as follows. A full overview including process activity descriptions is presented in Appendix C.

- **Requirement 1** Must unite participants around a collective problem that is made explicit.
  Achieved through Process activity 1, Process activity 2, Process activity 8, Process activity 9, Process activity 10.

- **Requirement 2** Should have a clear legal framework for information sharing.
  Achieved through Process activity 1, Process activity 8.

- **Requirement 3** Decisions should be reached collaboratively.
  Achieved through Process activity 2, Process activity 4, Process activity 9, Process activity 11.

- **Requirement 4** Must decrease the costs of sharing information.
  Achieved through Process activity 2, Process activity 7, Process activity 12.

- **Requirement 5** Should increase the individual rewards of sharing information.
  Achieved through Process activity 7, Process activity 9, Process activity 10, Process activity 12.

- **Requirement 6** Large communities could be organized in nested enterprises.
  Achieved through Process activity 5, Process activity 7, Process activity 9, Process activity 11.

Note that the 'leadership opportunities' of Chapter 6 are not included in this validation. Although the behaviour of the NCSC in the process does influence its outcomes, these are not activities that need to be undertaken but rather substantive recommendations of the author: they recommend the position which the NCSC should take *within* the interactive decision-making process.

Using this mapping, the governance design can be verified to indeed meet the requirements for improving information sharing. However, an important distinction must be made. While it can be established if the governance design meets the requirements, ultimately the outcomes of a process depend on the interactions between parties in the process and the results of their interactive decision-making.

Therefore the design of Chapter 6 being validated to meet the requirements of Chapter 5 does not guarantee improved cybersecurity information sharing in the National Detection Network. However, we can say that if the NCSC carries out the process activities and takes up the opportunities for leadership within the process, this is likely to result

in incentivization of the National Detection Network. The next section considers how the possible outcomes of doing so could be determined.

7.3.2 Validation

In the study a number of assumptions have been made. Some of these are reflected in the limitations of the approach, as discussed in Section 7.2. Other assumptions are more fundamental. While the design can be verified to meet the requirements, it cannot be validated if implementing the design would actually achieve the outcome of improving information sharing.

This section poses the question: Does the design solve the right problem? Does a collective action problem actually exist, and is it likely to be addressed by the design? In other words, validation is about confirming the outcomes of a design in its environment. In this study, the governance design has not been tested in the the National Detection Network, and therefore it is not empirically validated. By discussing assumptions, the uncertainties of the design can however be assessed.

First, the existence of a collective action problem. The study assumes that statements from the interviews could be trusted to represent the actual positions of organizations. That is to say, the observed discrepancy between ambition and practice of these organizations – that would be indicative of the existence of a collective action problem – might also be due to the 'polishing' of the ambitions as a form of organizational window-dressing. Although the author does not believe this to be the case it might explain the results, if not for the existence of a collective action problem.

Furthermore, the study assumes that an economic or rational explanation of behaviour applies: that organizations have the means or capacity to share but are unwilling to direct resources towards this. An alternative perspective from a field that considers irrational actors like psychology might have yielded a different finding, focused for example more on motivating individual behaviour of employees rather than considering their organization's interests.

The application of design solutions from the field of collective action is therefore theoretically perhaps not entirely sound, as was discussed in Section 7.2.1. As was motivated in Section 2.3, the pragmatic choice is made to consider cybersecurity information sharing as a collective action problem in order to explore avenues for solutions from this field.

An initial iteration of the design was discussed with domain expert Richard Kerkdijk of TNO in interview A.3.8. This provides some degree of feedback and validation, which was used in the iteration of the design proposed in this study.

Validation of the design could take place as follows. First, to improve the rigor of establishing a collective action problem, a larger group of participants than the eight of this study could be questioned on their interests and motivations to share cybersecurity information. This could be done using a questionnaire, possibly followed up with interviews. Organization's ambitions should be critically questioned and corroborated with their actions.

Second, the effects of introducing the proposed governance in the system could be validated by introducing it for a subset of the NDN participants and comparing sharing performance between groups. However, this would likely involve developing metrics for making sharing performance explicit also for the control group. Recall that metrics are part of the proposed governance. Measuring the performance of the control group might therefore already affect its sharing behaviour. This type of experiment is in fact already part of the proposed governance design: an initial trust group of motivated participants is used to test the approach and develop process agreements for consecutive groups.

Finally, validation of the proposed design could include a review of the effects on the broad aims of the National Detection Network, not just information sharing. As was

explained by an employee of the NCSC in interview A.1.1, aims of the NDN besides improving information sharing are to help these organizations build detection capability, to achieve situational awareness of cybersecurity threats, and to create CTI readiness at vital sector organizations. While Leadership opportunity 4 may contribute to capacity building, the broad aims of the NDN are not the topic of this study. Still, these goals could be impacted by introducing the proposed governance structure.

Overall, the results of this study may be used to inform future designs. However, the design should be seen within the context of the National Detection Network: the requirements and proposed design are influenced by the existing process (there is 'no green field'), they apply to the participants involved in the community, and are are situated in the policy landscape and culture of the Netherlands. More empirical research is necessary on the assumptions underlying the requirements and proposed design before they could be generalized to cybersecurity communities in a broad sense.

Chapter 8

Conclusions

The research questionof the study is: **How can information sharing in the National Detection Network be incentivized?** The NCSC can make collective goals of the NDN community explicit by involving participants in a process of interactive decision-making, where alike peers are motivated to share information in decentralized trust circles by instituting comparative reputational metrics.

A governance design of four phases is proposed by means of which the NCSC could transition the National Detection Network community to this state. This governance design meets the six requirements formulated in this study to improve cybersecurity information sharing: (1) it must unite participants around a collective problem that is made explicit, (2) it should have a clear legal framework for information sharing, (3) decisions should be reached collaboratively, (4) it must decrease the costs of sharing information, (5) it should increase the individual rewards of sharing information, and (6) large communities could be organized in nested enterprises.

8.1 Contribution

Fifteen years ago authors identified a free-rider problem in cybersecurity information sharing, and thirteen years ago the need to design incentives was first described in this field. This study adds to the limited but growing body of research on governance of cybersecurity communities.

Currently these communities are considered first and foremost as technological systems. No commonly accepted definition of a threat intelligence platform exists as of yet, and existing standards and institutions in cybersecurity communities are mostly induced from practice (e.g. STIX and the Traffic Light Protocol). This does however not address the issue of misaligned or missing interests that may exist in the communities.

Existing works that considers collective action theory and the role of organizational interests in cybersecurity information sharing do so in general terms, without analyzing the design implications stemming from collective action theory. This study identifies a knowledge gap on governance design with a collective action perspective in the field of cybersecurity information sharing.

The contribution of the study exists in a case study of the National Detection Network community based on interviews with 18 participants and domain experts, requirements for improving cybersecurity information sharing, and design for governance that operationalizes these requirements for the case.

The study hereby contributes an initial empirical basis for using the collective action perspective, which extends the now primarily technological works on design of threat intelligence platforms. The study takes a similar approach to Shiffman and Gupta (2013), who take a 'commons' perspective on cybersecurity information sharing. The study is

founded extends this theoretical work by proposing requirements and a design to improve information sharing in a specific community.

The results of this study could inform governance of other cybersecurity communities. However, the requirements and design proposed in this study should be seen in context of the National Detection Network. More empirical research is necessary on the assumptions underlying the requirements and proposed design before they could be generalized to other cybersecurity communities.

8.2 Relevance

Results of this work can be applied by the National Cyber Security Centre in order to improve information sharing in the National Detection Network. Information sharing may in turn lead to improved threat detection capabilities of participants. These capabilities contribute to an improved resilience of vital sector infrastructures and public organizations on which the citizens of the Netherlands rely, for example to handle financial transactions or deliver drinking water to their homes. Although indirect, this forms a very practical relevance.

Results of the study could be used to inform the governance of other cybersecurity communities, initiated by national governments or otherwise, in order to improve sharing of cybersecurity information. However, the requirements to improve sharing and proposed governance design should be seen in context of the case study of the National Detection Network, and be carefully applied beyond this.

The role of cybersecurity threat detection is becoming increasingly important, as traditional cybersecurity controls no longer suffice to protect against persistent attackers who are highly motivated or have abundant resources. Digital sabotage and espionage may have a significant impact on society if threat detection capabilities are not improved by sharing cybersecurity information. The study aims to contribute to a more resilient society through improving information sharing.

8.3 Future work

The perspective of collective action for cybersecurity information sharing should be seen as a starting point. The assumptions underlying the existence of a collective action problem in this domain could be empirically assessed by carrying out questionnaires and conducting interviews with a larger group of participants. Rigor would improve generalizability of the research results to other cybersecurity communities.

The effects of introducing the proposed measures for incentivizing cybersecurity information sharing could be validated in practice using a subset of the population. This approach is both practical and promising, as introducing interactive decision-making measures for a pilot group in the NDN community – referred to in the design as the initial trust circle – is part of the proposed approach. Care must be taken however when developing sharing performance metrics, as the mere act of measuring performance may also influence the sharing behaviour of a control group.

Besides verification and validation of results of this study, research could go out to the institutions and technologies mentioned in this work as possible means to increase trust between participants. These include metrics that accurately describe sharing behaviour in a cybersecurity community, and use of privacy enhancing technologies for sharing information between semi-honest parties.

References

Albakri, Adham, Eerke Boiten, and Rogério De Lemos (2018). "Risks of Sharing Cyber Incident Information". In: *Proceedings of the 13th International Conference on Availability, Reliability and Security - ARES 2018*, pp. 1–10. DOI: 10.1145/3230833.3233284. URL: http://dl.acm.org/citation.cfm?doid=3230833.3233284.

Allison, Pete and Eva Pomeroy (2000). "How Shall We "Know?" Epistemological Concerns in Research in Experiential Education". In: *Journal of Experiential Education* 23.2, pp. 91–98. DOI: 10.1177/105382590002300207.

Anderson, Ross et al. (2012). "Measuring the Cost of Cybercrime: a workshop". In: *Workshop on the Economics of Information Security (WEIS)*, pp. 1–31. ISBN: 9783642394980. DOI: 10.1007/978-3-642-39498-0{_}12.

Ben-Asher, Noam and Cleotilde Gonzalez (2015). "Effects of cyber security knowledge on attack detection". In: *Computers in Human Behavior* 48, pp. 51–61. ISSN: 07475632. DOI: 10.1016/j.chb.2015.01.039.

Bianco, David (2014). *The Pyramid of Pain*. URL: http://detect-respond.blogspot.nl/2013/03/the-pyramid-of-pain.html#!/2013/03/the-pyramid-of-pain.html.

Boeke, Sergei (2018). "National cyber crisis management: Different European approaches". In: *Governance* 31.February 2017, pp. 449–464. DOI: 10.1111/gove.12309.

Brown, Sarah, Joep Gommers, and Oscar Serrano (2015). "From Cyber Security Information Sharing to Threat Management". In: *Proceedings of the 2Nd ACM Workshop on Information Sharing and Collaborative Security*. WISCS '15. New York, NY, USA: ACM, pp. 43–49. ISBN: 978-1-4503-3822-6. DOI: 10.1145/2808128.2808133. URL: http://doi.acm.org/10.1145/2808128.2808133.

Bruijn, Hans de, Ernst ten Heuvelhof, and Roel in 't veld (2010). *Process management: why project management fails in complex decision making processes*. Springer-Verlag Berlin Heidelberg, pp. IX, 171. ISBN: 978-3-642-13940-6. DOI: 10.1007/978-3-642-13941-3.

Bruijne, Mark De, Michel van Eeten, and Wolter Pieters (2017). *Towards a new cyber threat actor typology A hybrid method for the NCSC cyber*. Tech. rep. Delft: Delft University of Technology, p. 71.

Burger, Eric W. et al. (2014). "Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies". In: *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security - WISCS '14*, pp. 51–60. ISSN: 15437221. DOI: 10.1145/2663876.2663883. URL: http://dl.acm.org/citation.cfm?doid=2663876.2663883.

Clark, Kas et al. (2014). "A Dutch approach to cybersecurity through participation". In: *IEEE Security and Privacy* 12.5, pp. 27–34. ISSN: 15407993. DOI: 10.1109/MSP.2014.83.

Compton, Jeff (2017). *The CTI Process Lifecycle: Achieving Better Results Through Execution*. URL: https://www.fireeye.com/blog/products-and-services/2017/10/cti-process-lifecycle.html.

Dandurand, Luc and Oscar Serrano Serrano (2013). "Towards improved cyber security information sharing". In: *Cyber Conflict (CyCon), 2013 5th International Conference on*. IEEE, pp. 1–16.

Dunn-Cavelty, Myriam and Manuel Suter (2009). "Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection". In: *International Journal of Critical Infrastructure Protection* 2.4, pp. 179–187. DOI: 10.1016/j.ijcip.2009.08.006.

Eeten, Michel van and Johannes M. Bauer (2009). "Emerging threats to internet security: Incentives, externalities and policy implications". In: *Journal of Contingencies and Crisis Management* 17.4, pp. 221–232. ISSN: 09660879. DOI: 10.1111/j.1468-5973.2009.00592.x.

Eeten, Michel van, Qasim Lone, et al. (2016). *Evaluating the Impact of AbuseHUB on Botnet Mitigation*. Tech. rep. Delft University of Technology. URL: http://arxiv.org/abs/1612.03101.

ENISA (2018). *Glossary*. URL: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary.

Fransen, Frank and Richard Kerkdijk (2017). "Cyber Threat Intelligence through National and Sector-Oriented Communities". In: *Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level*. Ed. by Florian Skopik. CRC Press. Chap. 5. ISBN: 9781138031821. URL: https://www.crcpress.com/Collaborative-Cyber-Threat-Intelligence-Detecting-and-Responding-to-Advanced/Skopik/p/book/9781138031821.

Fransen, Frank, Andre Smulders, and Richard Kerkdijk (2015). "Cyber security information exchange to gain insight into the effects of cyber threats and incidents". In: *Elektrotechnik & Informationstechnik* 18, pp. 106–112. ISSN: 0932-383X. DOI: 10.1007/s00502-015-0289-2. URL: http://link.springer.com/10.1007/s00502-015-0289-2.

Fuentes, José M. de et al. (2017). "PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing". In: *Computers and Security* 69, pp. 127–141. ISSN: 01674048. DOI: 10.1016/j.cose.2016.12.011.

Fulk, Janet, Michael Kalman, and Peter R Monge (1996). "Connective and Communal Public Goods in Interactive Communication Systems". In: *Communication Theory*. International Communication Association. Chap. 6, pp. 60–87. DOI: 10.1111/j.1468-2885.1996.tb00120.x. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1468-2885.1996.tb00120.x.

Gal-or, Esther and Anindya Ghose (2005). "The Economic Incentives for Sharing Security Information". In: *Information Systems Research* 16.2, pp. 186–208. DOI: 10.1287/isre.1050.0053.

General Intelligence and Security Service of the Netherlands (2018). *Annual report 2017*. Tech. rep. Zoetermeer: General Intelligence and Security Service of the Netherlands (AIVD). URL: https://english.aivd.nl/publications/annual-report/2018/03/09/annual-report-2017-aivd.

Gordon, Lawrence A, Martin P Loeb, and William Lucyshyn (2003). "Sharing information on computer systems security: An economic analysis". In: *J. of Accounting and Public Policy* 22.6, pp. 461–485. ISSN: 0278-4254. DOI: 10.1016/j.jaccpubpol.2003.09.001. URL: http://www.sciencedirect.com/science/article/pii/S0278425403000632.

Groves, Theodore and John Ledyard (1977). "Optimal Allocation of Public Goods: A Solution to the "Free Rider" Problem". In: *Econometrica* 45.4, pp. 783–809. ISSN: 00129682, 14680262. URL: http://www.jstor.org/stable/1912672.

Hansel, Mischa (2013). *Cyber Security Governance and the Theory of Public Goods*. URL: https://www.e-ir.info/2013/06/27/cyber-security-governance-and-the-theory-of-public-goods/.

He, Shu et al. (2016). "How would information disclosure influence organizations ' outbound spam volume ? Evidence from a field experiment". In: *Journal of Cybersecurity* 2.1, pp. 99–118. DOI: 10.1093/cybsec/tyw011.

Heuvel, Elly van den and Gerben Klein Baltink (2014). "Coordination and Cooperation in Cyber Network Defense : the Dutch Efforts to Prevent and Respond". In: *NATO Science for Peace and Security Series*. Ed. by Melissa E. Hathaway. Informatio. IOS Press, pp. 118–129. ISBN: 9781614993728. DOI: 10.3233/978-1-61499-372-8-118.

Hevner, Alan R (2007). "Scandinavian Journal of Information Systems A Three Cycle View of Design Science Research A Three Cycle View of Design Science Research". In: *Scandinavian Journal of Information Systems © Scandinavian Journal of Information Systems* 19.192, pp. 87–92. URL: http://aisel.aisnet.org/sjis/vol19/iss2/4.

Hevner, Alan R and Samir Chatterjee (2010). "Design Science Research in Information Systems". In: *Design Research in Information Systems: Theory and Practice*. Boston, MA: Springer US, pp. 9–22. ISBN: 978-1-4419-5653-8. DOI: 10.1007/978-1-4419-5653-8{_}2.

Hippel, Eric von and Georg von Krogh (2003). "Open Source Software and the "Private-Collective" Innovation Model: Issues for Organization Science". In: *Organization Science* 14.2, pp. 209–223. ISSN: 1047-7039. DOI: 10.1287/orsc.14.2.209.14992. URL: http://pubsonline.informs.org/doi/abs/10.1287/orsc.14.2.209.14992.

Hollingshead, Andrea B, Janet Fulk, and Peter Monge (2002). "Fostering Intranet Knowledge Sharing: An Integration of Transactive Memory and Public Goods Approaches". In: *Distributed Work*. Ed. by Pamela Hinds and Sara Kiesler. 14. MIT Press Cambridge, MA, pp. 335–355. ISBN: 0262083051.

Johnson, Christopher S. et al. (2016). "Guide to Cyber Threat Information Sharing". In: *NIST special publication* 800. DOI: 10.6028/NIST.SP.800-150. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf.

Joint Chiefs of Staff of the United States (2017). *JP 2-01 Joint and National Intelligence Support to Military Operations*. Tech. rep. Washington, D.C.: Department of Defense. URL: http://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/2-0-Intelligence-Series/.

Jongsma, Anton and JH Hoepman (2015). "Exchanging threat information between semi-honest parties". PhD thesis. Radboud University Nijmegen. URL: https://www.rijksoverheid.nl/documenten/publicaties/2014/03/17/nationaal-detectie-netwerk.

Kamp, Tim van de et al. (2016). "Private Sharing of IOCs and Sightings". In: *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security - WISCS'16*, pp. 35–38. DOI: 10.1145/2994539.2994544. URL: http://dl.acm.org/citation.cfm?doid=2994539.2994544.

Kerkdijk, Richard and Tommy Koens (2017). "Towards a mature cyber threat intelligence practice". In: *Innovating in Cyber Security*. URL: https://www.tno.nl/media/9419/innovating-in-cyber-security.pdf.

Laube, Stefan and Rainer Böhme (2017). "Strategic Aspects of Cyber Risk Information Sharing". In: *ACM Computing Surveys* 50.5, pp. 1–36. ISSN: 03600300. DOI: 10.1145/3124398. URL: http://dl.acm.org/citation.cfm?doid=3145473.3124398.

Mahmood, Tariq and Uzma Afzal (2013). "Security Analytics: Big Data Analytics for Cybersecurity". In: *2013 2nd National Conference on Information Assurance (NCIA)*, pp. 129–134. DOI: 10.1109/NCIA.2013.6725337. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6725337.

Mandiant (2018). *M-Trends 2018 Report*. Tech. rep., pp. 1–52. URL: https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html.

Meier, Roland et al. (2018). "FeedRank: A Tamper- resistant Method for the Ranking of Cyber Threat Intelligence Feeds". In: *2018 10th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, pp. 321–344.

MISP Project (2017). *Sighting the next level*. URL: http://www.misp.software/2017/02/16/Sighting-The-Next-Level.html.

Munnichs, Geert, Matthijs Kouw, and Linda Kool (2017). *Een nooit gelopen race*. Tech. rep. Rathenau Instituut. URL: https://www.rathenau.nl/nl/publicatie/een-nooit-gelopen-race.

National Coordinator for Security and Counterterrorism of the Netherlands (2018a). *Cyber Security Assessment of the Netherlands*. Tech. rep. The Hague: National Coordinator for Security and Counterterrorism, p. 76. URL: www.ncsc.nl%20https://english.nctv.nl/topics_a_z/csan/index.aspx.

— (2018b). *Resilient Critical Infrastructure*. Tech. rep. Ministry of Security and Justice of the Netherlands. URL: https://english.nctv.nl/topics_a_z/critical_infrastructure_protection/.

National Cyber Security Centre of the United Kingdom (2013). *Cyber-Security Information Sharing Partnership Terms and Conditions*. Tech. rep. August. NCSC-UK, pp. 1–16. URL: https://www.ncsc.gov.uk/cisp.

NCSC (2015). *Cybersecuritybeeld Nederland CSBN 2015*. Tech. rep. The Hague: National Cyber Security Center of the Netherlands, pp. 1–88.

NCSC-NL (2018). *Nationaal Detectie Netwerk*. Tech. rep., p. 1. URL: https://www.rijksoverheid.nl/documenten/publicaties/2014/03/17/nationaal-detectie-netwerk.

NIST (2014). "Framework for Improving Critical Infrastructure Cybersecurity". In: *National Institute of Standards and Technology*, pp. 1–41. ISSN: 0018-9219. DOI: 10.1109/JPROC.2011.2165269. URL: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

Olson, Mancur (1965). *The logic of collective action*. Cambridge, MA: Harvard University Press, p. 199. ISBN: 0674537513. DOI: 10.1007/978-3-319-20451-2{_}32.

Ostrom, Elinor (1990). *Governing the Commons: the evolutions of institutions for collective action*. Cambridge University Press, 298 pages. ISBN: 0 521405998.

Patcha, Animesh and Jung-min Park (2007). "An overview of anomaly detection techniques: Existing solutions and latest technological trends". In: *Computer Networks* 51, pp. 3448–3470. DOI: 10.1016/j.comnet.2007.02.001.

Poteete, Amy R, Marco a Janssen, and Elinor Ostrom (2010). *Multiple Methods in Practice: Collective Action and the Commons*. Princeton, NJ: Princeton University Press, p. 370. ISBN: 9780691146041. DOI: 10.2307/j.ctt3fgxrdM4-Citavi.

Sauerwein, Clemens et al. (2017). "Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives". In: *Proceedings of the 13th International Conference on Wirtschaftsinformatik (WI 2017)*, pp. 837–851.

Serrano, Oscar, Luc Dandurand, and Sarah Brown (2014). "On the Design of a Cyber Security Data Sharing System". In: *Proceedings of the 2014 ACM Workshop on Information Sharing #38; Collaborative Security*. WISCS '14. New York, NY, USA: ACM, pp. 61–69. ISBN: 978-1-4503-3151-7. DOI: 10.1145/2663876.2663882.

Settanni, Giuseppe et al. (2017). "A collaborative cyber incident management system for European interconnected critical infrastructures". In: *Journal of Information Security and Applications* 34, pp. 166–182. ISSN: 22142126. DOI: 10.1016/j.jisa.2016.05.005.

Shiffman, Gary M. and Ravi Gupta (2013). "Crowdsourcing cyber security: A property rights view of exclusion and theft on the information commons". In: *International Journal of the Commons* 7.1, pp. 92–112. ISSN: 18750281. DOI: 10.18352/ijc.343.

SIDN Labs (2015). *ENTRADA link for AbuseHUB*. URL: https://www.sidnlabs.nl/a/weblog/entrada-link-for-abusehub.

Skopik, Florian, Giuseppe Settanni, and Roman Fiedler (2016). "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing". In: *Computers and Security* 60, pp. 154–176. ISSN: 01674048. DOI: 10.1016/j.cose.2016.04.003. URL: http://dx.doi.org/10.1016/j.cose.2016.04.003.

Usoro, Abel et al. (2007). "Trust as an antecedent to knowledge sharing in virtual communities of practice". In: *Knowledge Management Research & Practice* 5.3, pp. 199–212. DOI: 10.1057/palgrave.kmrp.8500143.

Wagner, Cynthia, Alexandre Dulaunoy, and Andras Iklody (2016). "MISP - The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform". In: *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, pp. 49–56. DOI: 10.1145/2994539.2994542.

Weber, Steven (2000). "The Political Economy of Open Source Software". Berkeley, California.

Wenger, Etienne and William M Snyder (1999). "Communities of Practice: The Organizational Frontier". In: *Harvard Business Review*, pp. 139–145.

Terms and abbreviations

CERT Computer Emergency Response Team. 14

CTI Cybersecurity Threat Intelligence. 12

FOIA Freedom of Information Act, Wet openbaarheid bestuur (Wob). 20

IDPS Intrusion Detection and Prevention System. 11

IDS Intrusion Detection System. 29

IoCs Indicators of Compromise. 11

ISAC Information Sharing and Analysis Centers. 15

SOC Security Operations Centre. 11

STIX Structured Threat Information eXpression. 13

TLP Traffic Light Protocol. 16

TTPs Tactics, Techniques and Procedures. 17

Wgmc Wet gegevensverwerking en meldplicht cybersecurity. 36

Wiv Wet op de inlichtingen- en veiligheidsdiensten. 36

List of Figures

List of Tables

Appendix A

Interviews conducted

A.1 NDN system owners

A.1.1 An employee at the National Cyber Security Centre of the Netherlands (NCSC)

04-06-2018

The ambitions for the National Detection Network are threefold. First, to contribute to resiliency of organizations in the Netherlands by exchanging threat intelligence and by helping these organizations build detection capability. Second, to achieve situational awareness of cybersecurity threats. Third: to create CTI readiness at vital sector organizations. The goal is for the NDN to facilitate about 300 organizations in exchanging threat intelligence bidirectionally.

The current NDN is based is on classic internal network monitoring. When I was first involved in 2012 the aim was to do network detection at government organizations in order to create a feedback loop for what back then was still called GovCERT. Realizing a pilot project for even a passive honeypot detection system proved hard, due to a lack of legal framework, financial constraints, and uncertainty on how to deal with the possibility of coming across personally identifiable information.

In 2012 a cooperation with the AIVD and MIVD was started. The NCSC had 2.5 FTE working on the NDN, with progress existing mainly of addressing important preconditions for doing network detection in government systems. For example, for two years we had meetings with various employee councils ("ondernemingsraden") of the involved organizations in order to address privacy concerns. Eventually we decided on a sensor network in government organizations and exchanging events using MISP.

After the successful pilot project for government organizations had commenced, the NCSC decided to engage private vital sector organizations in a parallel project. We started with 8 organizations that were ahead in terms of cybersecurity maturity. As we believe strongly in cross-sector sharing, these included an ISP, an energy producer, an a financial institution. A series of roundtable discussions with these organizations was organized in order to decide on what the NDN should deliver and how the cooperation should be developed. Here the decision was made to work towards sharing back sightings. However, the NCSC had lack of capacity and little progress was made in terms of development of the technology and improving quality and relevance of the CTI. For the more mature participants, this caused a decrease in interest in the roundtable meetings and reduced participation from the parties in sharing CTI and sightings.

Currently participating in the NDN are some 20 vital sector organizations and 40 public organizations with hits on indicators now being reported primarily by sensors at public organizations. These numbers are steadily growing. No organizations have left the group. As for exit rules, we have formulated conditions with private organizations. Apart from participants, there is a flexible group of stakeholder experts who contribute to the NDN. To deliver relevant CTI it is necessary for the NCSC to have a good understanding of the assets and risks of the NDN constituency. For private organizations, possible barriers to sharing sightings might be reputational risks and costs. For public organizations, important preconditions lie in ensuring privacy and compliance.

The desired effects of the NDN for our organization are twofold. First, the NCSC needs to be aware of threats and attacks over time. Second, the NCSC should be able to provide valuable information for organizations to improve their resilience. Over time we have noticed that this aim is wider than originally believed: to be successful we need to go beyond delivering CTI in a technical system. For example, increasing resilience in an organization is possible only when preconditions like technological maturity and top-level support are met.

Currently private organizations involved in the NDN fall in a single group, but companies need a business-case to invest in bilateral knowledge sharing and sharing sightings. Therefore we are considering moving towards a 'bespoke' model: creating groups of highly and less involved parties, which exchange information based on their needs. This would provide an incentive for active participation, as this would give access to levels of increasingly valuable CTI.

Actors and stakeholders in the NDN have not influenced the aims of the system much. Early in the process there was an organized discussion ("klankbordgroep") with the participants on managerial level on the aims of the NDN. In hindsight, this was too early as there had been not enough progress made at that point. Many companies seem happy to follow our progress on the NDN and remain passive when asked to engage. It seems to me that as the network effects increase with more participants, actors will become more eager to be involved in decision-making on goals and means of the NDN. The NCSC would welcome this type of involvement.

Examples of strategic behaviour have occurred between partners of the NDN, where each continually assesses: is it in my interest to continue with the project, and how can it contribute to my other goals? We also see some of the more mature participants in the network behaving strategically. They see the NDN primarily as a way to get CTI without compensation.

The interviewee was asked to respond to the elements of process design according to Bruijn, Heuvelhof, and 't veld 2010.

The NDN project is owned by the NCSC. An important signal was when the Minister of Justice and Security, responsible for the NCSC, briefed Parliament on the NDN. The NCSC therefore decides on the direction and tempo of the project, period. New participants are able to enter the project if we agree that it would be relevant.

When it comes to respecting core-values, I believe there currently is an imbalance: the NCSC considers interests of other parties and how to address them, while this isn't reciprocated. This imbalance is understandable and acceptable, as we have means and staff dedicated to reaching out to these organizations. We should nonetheless attempt to show our interests in the NDN better, as it will turn out that addressing this by increasing sharing would not cost the participants much effort.

If I had to describe the cooperation between partners in the NDN in three phases they would be: (1) constructive beginnings, (2) commitment but little progress meant partners had little to show for, (3) in the current phase a clear need to make progress. This urgency and ability to speed up progress is related to the €12.9 mln that Dutch government has invested in cybersecurity yearly ("versterkingsgelden in coalitieakkoord"). We now notice that operational cooperation is also possible.

It is mostly the NCSC that attempts to keep up momentum in the project. Many participating organizations are not thinking about the NDN on a daily basis. We may have lost interest and engagement from some early participants, but I believe this can be won again by showing progress.

As for substance, conceptually there is very much place for new ideas and contributions. However, structurally we have now made certain decisions that are fixed, for example for a certain type of sensor, CTI providers, and threat intel platform.

A.1.2 An analyst at General Intelligence Service of the Netherlands (AIVD)

18-06-2018

The interconnectedness of digital technologies and the national interests of the Netherlands leads to a role for the AIVD in protecting the Dutch legal order through cybersecurity.

The National Detection Network started with pilot projects for threat detection in 2013. The landscape has since changed and the potential support for the NDN has increased. First, the geopolitical circumstances have changed with campaigns becoming more serious. Second, the Netherlands has a new legal framework with the Wgmc, BIR, and Wiv. Third, political awareness has increased.

The National Detection Network has become a 'brand name' for a series of collaborations and should be seen as separate from the delivery mechanisms for CTI employed. More important than the delivery mechanism is the continuous cooperation between NCSC, AIVD and MIVD as well as partners in the NDN as with their constituencies, all within their legal tasks and their legal frameworks. There exists an ongoing discussion on the nature and scope of the NDN. It could encompass the sensors, information products, security advice , incident response or all of these in some form. Now that the pilot projects have ended it is time to grow towards a more mature NDN in terms of infrastructure and processes.

We view the NDN as a cooperation in which AIVD and MIVD focus on state-level actors and the NCSC is responsible for other threats. In practice these lines are often blurred due to the issue of attribution. Future cooperation will have to show where the greatest added value and responsibility of each organization lies.

Cooperation is not a goal in itself. The goal of the NDN should not be to exchange more threat intelligence, but rather to offer more suitable prospects for action ("handelingsperspectief") to targets of threats, for which the exchange of threat intel could be one of many means. Exchange of information could be done using the NDN infrastructure, via the NCSC, or in direct contact with a target. As intelligence service we could choose to bypass the NDN infrastructure and/or NCSC for reasons of need-to-know and source protection. Ideally we help organizations improve their own security, and threat intelligence is just one of the means to do this.

Our threat intelligence is often high in the pyramid of pain, i.e. revolving around tactics, techniques and procedures of adversaries. However, threat intelligence will be classified when it was acquired using special investigative powers ("speciale inlichtingenmiddelen") of the AIVD. We can sometimes share the derived lower-level threat intelligence such as IP's or hashes. We will not share classified information in MISP, because MISP does not comply with our security standards for the exchange of classified information. We aim to use delivery mechanisms using the STIX/TAXII standards.

A.2 NDN participants

A.2.1 A strategic security specialist at Bank 1

26-04-2018

As a financial institution we are a target of interest and need to be resilient to attacks. We have improved on a baseline level of security by exchanging tactical threat intelligence (Modus Operandi) within the FI-ISAC. Parties in the NDN have expressed the ambition to extend this to operational threat intelligence. The end goal for both tactical and operational threat intelligence is reducing risks. Hence for my organization I'd be satisfied

when if NDN manages to help us to reduce risk and stay in bounds of the risk appetite as defined in broad terms for operational risk management in a cost effective manner.

In my role as representative at the FS-ISAC I became involved with the NDN in the roundtable meetings during the initiation-phase, when we decided to expand the system from a government initiative to the vital sector organizations. For financial institutions, the NDN was a useful approach to develop the necessary instruments for exchange of operational threat intelligence. In addition, the NDN was perceived to offer information from intelligence sources that could otherwise not be acquired.

The four largest Dutch banks were already sharing operational intelligence before the NDN in a limited sense at this point by exchanging and blocking transactions from bank account numbers of 'money mule' launderers. Over the last few months the three large banks in the Netherlands have increased cooperation through Finance CERT where representatives of their SOCs structurally meet, and SOC processes are aligned. It is the ambition to also start exchanging CTI in this context.

The goal of the NDN is making the next step in exchanging knowledge and experience. In the FS-ISAC we already exchange on a tactical level the observed threats. The NDN will help to on an operational level exchange the data corresponding to a threat.

There are limited resources we can allocate for security, we are very understaffed. At the same time, a possible advantage of the NDN in terms of costs would be that it prevents organizations doing work twice. Gathering and interpreting CTI could well be done collaboratively, which leaves more resources to focus on the response.

Currently CTI sources we are using don't have a focus specific to the Netherlands. The added value of the NDN lies in receiving information that we cannot get from other sources. The first is CTI from intelligence agencies. In the past we've also been asked to exchange CTI with the agencies outside of the NDN, which made this added value less clear. The second is information from sightings reported by other parties in the NDN, which would indicate the urgency of a threat to our organization. In this sense, sightings would increase the value of CTI through coupling between high-level CTI and low-level IOC's.

A barrier to reporting sightings lies in automation, the demand which reporting sightings puts on our resources. I am confident that the correct agreements and techniques can guarantee the confidentiality of data and sharing hits does not violate our business interests. Sightings would need to be reported timely for the information to have value, at least once per week or more.

The NDN could improve detection of cybercrime on a national level, by offering a view of the entire kill chain. Banks are located at the end of the kill-chain and might therefore process illegitimate transactions, which are the result of an attack at another organization earlier in the kill chain. By sharing CTI we collectively have a higher probability of detecting attacks.

The NDN has not achieved its goals yet. Over three years we've worked towards finding the right instruments. Now that the NCSC offers a MISP instance our organization is not yet equipped to connect to this. Perhaps it would be better to work with a full cloud-based system so that organizations making use of the NDN would need only a SIEM. In addition, we've experimented with EclecticIQ for more high-level threat intel but are now using a different web-based system that makes it easier to connect external threat feeds.

Most people within our organisation see the value of sharing CTI. However not everyone is convinced yet that NDN is the party that is able to deliver that. I think the best to overcome this type of resistance is to have participating organizations show the added value, and through automation reduce the barrier to participating.

A.2.2 An operational security specialist at Bank 1

26-04-2018

Customers want secure banking in their own financial interest. When my department identifies a threat timely we can prevent incidents. We use a SIEM, IPS, IDS, anti-DDOS systems. We don't use the NDN much. Commercial alternatives are better for collecting CTI, and when sharing CTI in the NDN we have noticed a lack of response. When we shared our own analysis of a previously unknown phishing attack, we did not get feedback from the NCSC or peers. This may be due to overlap with other forums where we share information, in this case a mailing list of peers. Here we did receive feedback.

The participating companies are of the Dutch vital infrastructure, but I'm missing a lot companies in the NDN. I haven't used the system in a long time. We might be more interested in using NDN when there is a possibility to automatically exchange IoC's.

NDN does not currently achieve its goals. Commercial alternatives are days faster and provide more information. The NDN is localized too much in the lower level of the pyramid of pain, while it should be in the higher-level TTPs.

By sharing knowledge we can together increase detection. Partners in a sector can enrich IOCs. Sightings should be shared in real-time. This is one of the hard aspects of the NDN, but can also provide greatest value as IOCs are very volatile. It is hard to identify why we don't share sightings, possibly due to a lack of interaction and feedback. It is hard to identify beforehand what type of feedback should be provided by the NCSC.

Of the intelligence services it is well known that they collect CTI but often don't share back.

I expect many large banks will share our views. Smaller organizations or banks without a SOC might derive more information from the NDN than we do.

A.2.3 A strategic security specialist at Bank 2

30-04-2018

The product of a bank is trust. We therefore need to understand our risks and threats well. We do our security in-house and provide monthly reporting for our CISO and other colleagues on current risks, including APTs, sectoral threats, and threat intelligence.

An interesting question to ask is: what is threat intelligence exactly? It could be as diverse as simple indicators, doing analysis on these indicators, or enriching the indicators before providing them to a participant.

We have many CTI feeds in our organization, including packaged with our SIEM, firewall, proxy, endpoint protection. Then there are the FS-ISAC and NDN. Currently we use the NDN mostly as a supplier of indicators. The FS-ISAC feed consists of some 300 emails per day, which is hard to automate in your detection processes.

The CTI in the NDN is now very operational, located in the bottom of the pyramid of pain. You want it to be higher, in the TTPs. This is more interesting because TTPs are more persistent for an attacker over time, but also because they have a lower false positive rate. This layer seems hard to automate but is more interesting to us.

Lower-level CTI should be automated using standards, but it needs to be higher quality than currently. And higher-level TTPs could well be offered as reports to aid threat hunting efforts. These reports could be rewritten as indicators by us.

The goals of the NDN are the same as the goals of the NCSC, the NDN is just one of their tools. On the position of the NDN we've always been told: "We want to offer information that others cannot, very specific to the Netherlands. Not a lot of events but high quality."

In general we deal with a lot of noise in CTI: false positives, outdated information. We expect and indeed see the NDN delivering higher quality data than some of our other sources, where the false positive ratio is so high it becomes hard to extract the relevant information.

Reporting of sightings is an important part of closing the feedback loop. They could be used to increase data quality by validating events. Sightings should also lead to more focus with threats offered that are specifically relevant to the Netherlands.

The most important factor here for us is that sightings on our network shared with the NCSC and others cannot be related back to our organization, for example through Wob-requests to the NCSC. So it's an issue for our legal department.

From the technical perspective we do not mind sharing indicators as long as this does not cost my analysts too much time. Interconnection costs are usually less of an issue: in cooperation with other banks we often exchange knowledge and code on this. If the NCSC wants more organizations to report sightings it might consider an effort to connect them.

Our threat intelligence platform uses the STIX/TAXII format and cannot exchange MISP events. I understand from my colleagues who use the system that there is now some authentication problem with the NDN MISP instance.

We have not shared a sighting before as we don't have hits. However, negative results might also be interesting to share. Some years ago we attempted to share CTI stemming from our own research, but the NCSC did not seem to know what to do with it.

I expect banks stand on these issues mostly the same. Differences between sectors are likely larger.

A.2.4 A security analyst at Bank 2

30-04-2018

As part of the Cyber Defence center, my responsibilities are for our infrastructure. Our aim is to ensure that our customers can do their banking in a secure way. Having a good reputation in this field is important for our organization.

Threat detection will definitely play a large role in our security architecture, but we are still in the process of determining what we want to do with threat intelligence. For example, we have endpoint protection with IOC hashes supplied by the vendor.

In addition, we use the Soltra Edge threat intelligence platform as recommended by the FS-ISAC and then import feeds from FS-ISAC and Fox-IT. We then push these feeds to our SIEM and see if we have hits.

With an average false positive rate of over 90% on over 10 hits per day, we have disabled notifications on our SIEM as it was becoming unworkable.

I have not worked with the NDN, although we do receive security advisories from the NCSC. Looking online for NDN yielded only two paragraphs of general information on the NCSC website. Based on this, it seems to me that the goals is to share IOCs within a community using STIX/TAXII.

The value of the NDN might exist in having a lower false positive rate, as well as supplying timely information. Filtering by sector would also be a nice to have feature.

Reporting back sightings on our network would have to be anonymized and automated. It could also be used to further decrease the noise rate. There is a slight barrier in creating the connection with our SIEM, but doing this would decrease the overhead significantly.

Standards are important for us. The NDN uses MISP, others email us with PDF attachments. We prefer the STIX/TAXII standard.

A.2.5 A strategic security specialist at drinking water company 1

07-06-2018

Cybersecurity is important for our organization, as processes have become increasingly digitized. The primary asset for our company is the Operational Technology, which generates, produces and delivers drinking water to homes. An additional important asset as well is the personal data of our staff and customers.

Threats include people who pursue financial or ideological gains (e.g. by holding information or infrastructure ransom), as well as terrorist and state-sponsored groups. We've noticed an increase in spearphishing and CEO-fraud. For our organization, digital attack vectors might be harder to exploit than other vectors. Espionage threats to drinking water companies are currently limited, as we don't have much intellectual property or many competitors.

We don't have a SOC, cybersecurity is a shared responsibility between multiple teams. We use a layered network architecture with detection capabilities at various places. Security providers feed these systems. We have a dashboard to monitor the various event sources. Our network is segmented logically between IT and Operational Technology.

We share information in the Water ISAC for the Netherlands using email, telephone, and a Sharepoint portal for more sensitive information. This is working fine for our information needs.

The most useful information for us is high-level CTI, but I foresee that when we move towards automated detection there will be a need for actionable low-level IOCs.

We currently use a 'light version' of the NDN in order to know what our peers are seeing and to receive indicators. We receive events but use them in a limited way: we attempt to monitor events, and for events with status exceptional we try to respond. Events in the NDN are timely enough for us, while we use the NCSC advisories after the fact to validate our response.

Collecting IOCs from the NDN is good, but keeping the NDN top-of-mind is hard while reporting sightings is complex. The interface for reporting sightings in the NDN is not working well. We report sightings manually, i.e. in the MISP web-interface. We want to connect with the NDN in an automated way in the near future.

We've received training from the NCSC on how to use the NDN, but there is not a good way to report back on existing sightings in NDN. It is impossible to report that a sighting was not found on our networks. If organizations could easily share results of sightings, the NDN would become more interactive and lively: a two-way exchange.

If sightings and other contributions to an event would be related to the respective events, instead of being added to new events, this would improve the quality of the data. This would hopefully also lead to fewer email notifications. It would be helpful if I would be able to change my email settings, for example for 'generic' type events.

You should consider speaking to drinking water company 2 as well, considering that they are ahead of us in terms of NDN-automation and monitoring dashboards.

A.2.6 An operational security specialist at drinking water company 1

07-06-2018

We have a vital function in Dutch society and need a fast and simple way to see when somethings is wrong in terms of cybersecurity. Inside drinking water companies there is not enough attention and resources for security, but I expect this will change if a large incident happens.

I'm responsible for the ICT infrastructure team, which exists of ten people. We do all servers, networking, and security. One employee works on security full-time.

We use endpoint security and an IPS. We have a number of firewalls and are building active monitoring capabilities on those. We don't do this yet due to capacity problems. Yearly we conduct a penetration test to determine if our network is segmented well, as

well as crisis preparation in which ICT is always a component. We don't use a SIEM solution as of yet.

It is important to keep in good contact with peer organizations, to help each other make choices in how to deal with threats. We do this in the water-ISAC, and with the NDN. We share information in the water ISAC, through for example conference calls.

We don't share much in the NDN. The system is complicated and it is sometimes unclear what to make of all the information contained in it. You see CSVs, port numbers, responses by others, while all I really want to know is: what should I pay attention to first?

We have contributed occasionally from our own research to events of others, but so far we've never shared an event. We don't use the system enough, I log into the portal maybe once or twice per month. The interface makes the system hard to follow, and it is hard to create a new event so that others can actually use it: what boxes to tick, what colors to apply? It would take us a lot of documentation before we could actually contribute.

Me and two colleagues visited the NCSC for a training on the NDN. However, during the tutorial on the tool not everybody was able to keep up with the tempo due to the complexity, even though we are interested to learn about the system.

We don't use a SIEM as of yet, but would be interested to start using the NDN in an automated way, for example to let us receive the high/high events in a dashboard. I see many organizations struggling with setting up SIEM solutions, perhaps the NCSC could help in making a choice or offer a 'shared SIEM'.

During the training there was brief attention given to the fact that an API exists but this lacked practical follow-up: the link offered did not work, so we emailed back and forth and over time got stuck. A more active approach from the NCSC would be welcomed.

You don't hear enough about the NDN. We've been to the training, but after that you just receive a lot of system emails and that's about it. I would welcome a more active discussion with other participants maybe once every quarter on problems people are having and the direction of the development of the NDN.

We could learn a lot from what larger organizations are experiencing. I see the potential of the NDN, but currently it is always the same people who are contributing to the portal. I believe there is a lot to win here.

A.2.7 A security specialist at drinking water company 2

04-07-2018

Delivering drinking water is our primary goal. We have physical assets that support this. We have determined the level of acceptable risk in terms of hours of unavailability of our IT systems and loss of data. Making risk explicit enabled us to gain top-level support for a security roadmap.

It is important to recognize to understand that a baseline of proper infrastructure architecture and standards is a precondition for improving security. Between 2010 and 2016 we have improved our network and systems and taken preventive measures. Since 2016 we've been working on real-time detection and information exchange.

We use a layered defense, and our IT network and operational network are physically separated. We use a dashboard for monitoring operational technology disruption alerts. We monitor the network for anomalous data flows and conduct vulnerability scanning.

We use strict rules for the inner networks, where for example all USB ports on operational systems have been disabled. For assurance, we conduct quarterly internal audits and regular pentests. Security awareness is a priority for our organization. We enforce clean-desk policies and have regular training sessions.

We conduct network monitoring inside the network and outside our firewall. To analyze events, instead of an off-the-shelf SIEM we use a data analytics tool to pull in data from various points in our organization, e.g. from our ERP system. This works well for our needs and is more affordable than a full-blown SIEM. Threat intelligence sources we use are the National Detection Network, Cisco as part of other products, and the free AlienVault open threat exchange.

The NDN is our primary source for two reasons: validation of information by the Dutch intelligence services ("inlichtingen- en veiligheidsdiensten"). And second, relevance for the Netherlands and vital sector organizations.

We appreciate that NDN event offers actionable information on mitigation. When the NCSC recommends certain detection rules, these are inserted in our IDS automatically without requiring confirmation from us. We do not do this for other threat intelligence sources. Because of the NDN we do not need our own team of threat intelligence analysts.

The timeliness of information in the NDN is sufficient for us. We prefer reliable intelligence over fast delivery. However, even if you trust your intelligence sources you still need redundancy to ensure you do not miss essential information, this is why we use other sources as well.

In 2016 we started cooperation with the NCSC and our management made the decision to want to be a sector leader in NDN development and take a role as an ambassador of the system. Already in 2016 we made a real-time connection with the NDN, and were able to do two-way exchange of intelligence. The initial costs of connecting with the NDN were around €15.000.

We have been a proponent of automated sharing back of information. The reason for this is that our organization is dependent on other critical infrastructures: an outage of the electrical grid would for example mean that we could not meet our goal of delivering drinking water. Therefore we should share information between sectors to improve security overall.

Ideally the collectively shared sightings would enrich the existing events in the NDN. We do not need management-summaries of threats, as we prefer to do our own reporting based on data in the NDN.

However, we want to share more than is currently possible. First, we would like to be able to report sightings for hits as well as non-hits, i.e. when we scan for an indicator we want to be able to share when it was not found, as well as when it was found. Second, we want to be able to do this for two sensors: outside our firewall and inside our network. And third, we want to be able to report sightings for indicators coming from sources other than the NDN.

When I proposed this type of sharing sightings at a meeting of NDN stakeholders on 9 October 2017, it was met by resistance from other organizations. Perhaps it is because we've taken a leading role in the NDN, but I feel like the sense of community ("samengevoel") is not arising in the NDN. From the interactions with other NDN participants, I often get the sense that they do not have the necessary baseline of infrastructure architecture to conduct network monitoring.

We have also made our desire for this type of sharing known with the NCSC, who responded enthusiastically. This was on 5 October 2017. However, to date we have not gotten a conclusive response on the suggestions. In January I reminded the NCSC of our proposals for sightings and spoke with a developer of the NDN platform, who told me that at this point the type of sharing back which we proposed was not possible but that they would consider developing it. I would like to know at this point: will the NCSC use our ideas or have they chosen a different route?

If I were in the position of the NCSC, I would take a more active approach. I imagine the NCSC must have been having capacity problems since October, but I would have

appreciated some timeline for when we could expect feedback. Our organization considers itself an ambassador of the NDN, but to be honest I could not tell you anything new about the NDN as compared to one year ago. We would like to know the status of the NDN: what is currently the focus of the NCSC, and what is the product roadmap?

Another feature I would like to see in the system is test-events, so that I can confirm that our monitoring systems are functioning well.

Decisions about the future of the NDN should happen with a small circle ("en petit comité") of engaged organizations. We would be happy to follow up to these decisions and contribute to development of the platform.

A.2.8 Hans Bos, Head Security Centre at Rijkswaterstaat

11-07-2018

The assets of Rijkswaterstaat include tunnels, bridges, dams, flood barriers, and road signaling systems. In addition, we protect informational assets that support our physical assets and inform the citizens of the Netherlands. As industrial automation has become more important for our sector, so has digital security.

Rijkswaterstaat has a security operations center and a security by design team. The first is responsible for day-to-day monitoring, the latter for design of safe systems and producing in control statements for the Dutch Court of Audit ("Algemene Rekenkamer"). I manage the teams, which together have some 20 FTE.

Our SOC has five functions. First, monitoring and response. Second, threat intelligence. Third, forensic research. Fourth, penetration testing. Fifth, guarding baseline security. All these functions are connected to our ICS/SCADA and information systems.

The primary tooling of our SOC is a SIEM system. We use IDS with threat intelligence feeds from our IDS vendor. Furthermore we develop IoCs in the field of ICS/SCADA and provide these to the community via NCSC. We have a single NDN sensor. However, I need many more to adequately cover our physically wide network, which spans over 3000km.

Therefore, in addition we have third-party sensors that make use of event filtering based on machine learning. These are tuned specifically for our important assets. The vendor of these sensors is fast in responding and continually develops the sensors on-site. These sensors give us awareness over out network and a high level of control over information flows.

By contrast, the NDN is a black box. There is a high level of secrecy at the NCSC and we do not know what are the inputs or outputs of the sensor in our network. We receive official notices ("ambtsberichten") directly from the AIVD through other channels than the NDN, but I assume that the AIVD also feed the NDN sensor with detection rules.

We are in the Threat Intelligence Platform pilot project of the NDN. During the initiation phase we recommended the NCSC to set up a centrally hosted system, but they chose for self-hosted. We have not succeeded in making the platform operational at Rijkswaterstaat so far, as we've run in to internal problems as concerned deviating from technical standards for this project, which takes time to gain permission for.

For now the NDN TIP platform therefore has no value for us, other than learning what you experience when doing things in collaboration. I see how it might be of value for our SOC, but even when it becomes operational an analyst at Rijkswaterstaat would still be necessary to translate threat intelligence from the platform into detection rules specific for our assets. These are the kind of barriers you encounter when being at the forefront of such developments. We understand this, and will continue putting effort in the NDN TIP platform.

I believe the importance of exchanging threat information is evident. It is strongly tied to security of the Netherlands. You have to share in order to advance as a whole.

Already in 2014 we took the initiative to start sharing incidents on our networks with the AIVD and NCSC, who at the time found it hard to use this information.

I would be proponent of strong cooperation between the NCSC, AIVD, and vital-sector organizations. My concern would be that collaboration could become too political for the governmental organizations and they will raise avoiding political risk above achieving results. At an operational level however there is a strong will to go for collaboration.

A.3 Domain experts

A.3.1 A CTI analyst at Deloitte

15-05-2018

During my 1.5 years at Deloitte I've worked on threat landscaping and CTI analysis, writing reports for clients on cybersecurity threats. These clients want to anticipate possible incidents, and we help take preventive steps, bring focus, and when necessary resolve an incident.

Our clients are often enterprises, coming to us is to protect business processes and intellectual property. They have varying degrees of detection capabilities and are looking for a high-level overview of threats based on a set of keywords for their organization. Tailored reports and recommendations we deliver weekly to the client CISO. In the report we describe IOC's and possible mitigation, but try not to get too technical as the reports needs to be understandable at the strategic level.

We base our work on open source intelligence, social media analysis, and the darkweb sources where malware is initially offered. In addition, we subscribe to a FireEye threat feed and share IOC's from this feed with our clients.

Mutual confirmation of events can be extremely valuable information for private organizations. I know the financial sector is making good progress in sharing CTI. We always recommend our customers to share threats and IOC's with their competitors. This could take the form of a physical face-to-face weekly meeting, although I am unsure if clients have ever taken up this advice. Real-time sharing of events would be best, but we have not recommended building a platform to our clients as this would come at too large a large financial burden.

When it comes to the NDN, I am interested to see where it will go. It seems that establishing trust and validation of CTI in the NDN will be an important factor, as in my experience it takes years to build relationships in an offline setting. Security of the platform will be extremely important, or organizations will not want to share their relevant CTI. Sharing with a government party might also be by itself problematic for some private organizations.

For a threat intel platform I don't use MISP myself, instead I use Alienvault and ThreatConnect. This is useful for tracking threat actors over time, although you always have to be sure to critically assess information in open-source CTI sources. For example by checking how many analysts have worked on a piece of information.

A.3.2 A security manager at an AEX-traded high-tech company

25-05-2018

Intellectual property is central to our business. It is necessary for my organization to protect this IP in order to retain our R&D efforts. In addition, we need to guard business continuity of a highly controlled fabrication process.

My organization has a IT competence center for IT security. I lead the Cyber Defense Operations Team, responsible for security monitoring and incident response, vulnerability

management, and threat information and dissemination. Our SOC of twelve persons is outsourced as a service, and we have an in-house CSIRT team of five persons in-house that handles events escalated by the SOC. Our organization has some 20.000 employees overall.

As part of monitoring and response we require a good view of the threat landscape, both for daily response operations and for continually designing our monitoring capabilities. To this end we use internal threat intelligence by logging events and cases, although we don't currently extract indicators and artifacts that could be correlated over time.

In addition we use external threat intelligence, which we buy from commercial providers and also receive from informal and formal trusted communities. An example of the former is sharing between heads of CERTs, an example of the latter is the multinational-ISAC of the NCSC.

The commercial sources we use contain three types of information. First, we receive high-level trend descriptions and identification of threat actors and campaigns. Mostly this information is repackaged in a periodic email we receive, with sometimes proprietary information added by the vendor. As consumer of this information it is hard to evaluate its completeness and value.

Second, we receive intelligence for vulnerability management. We have such a diverse landscape that making an overview ('photo') of the systems at our organization is not feasible and therefore we use this in a limited way.

Third, there are the IOCs which are de-duplicated and prioritized by our feed provider, as part of the SOC-services we purchase. We receive contextual information, like temporality and confidence on the events. This is entered into our SIEM, and used actionable in the SOC.

In terms of quantity the category of IOCs is the largest, but they are low in the pyramid of pain and quickly lose their relevance. Potentially the most valuable information would be our internal threat intelligence derived from events on our network, but while we collect logs we don't extract this information often. After this, the strategic information is valuable. Unfortunately for us, most commercial threat feeds over-represent financial institutions and government organizations, as these are their primary customers.

We are part of the multinational-ISAC, which provides small benefits to us. The group of organizations is not based around a sector, so intelligence remains generic. And it is disseminated quite slowly through the CISO level, as meetings happen once every six weeks or so.

Some information and best-practices are exchanged by us bilaterally with high-tech organizations, but also this remains often quite generic as there are not many companies with our specific profile.

To address this, we are in the process of forming a regional security community of high-tech companies and local suppliers, similar to communities for Schiphol and the harbour of Rotterdam. This is based on a regional shared function that is not reflected in intelligence from the NCSC or commercial CTI providers. Eventually the regional security community could exchange CTI in an automated way, for example through a shared MISP system or using STIX/TAXII.

Automated sharing of sightings could deliver potentially very useful information, and once set-up would not require much maintenance. The biggest hurdle to this would be the perceived risk of reputation damage. We cannot accept the risk of a severe incident inside the organization being leaked to outside the community due to knowledge-sharing.

We have engaged with the NCSC in an earlier stage on possible participation in the NDN. An important question in this for my organization is what information would need to be exchanged, and what safeguards exist. What access would the NCSC need to have, and what is the legal framework? Especially when formalizing the collaboration, our legal

and IP departments would need to become involved. This makes collaboration in the NDN much harder than interpersonal information-sharing in for example an ISAC. We do not feel the need to become involved in the NDN again at this point.

A.3.3 Jaap-Henk Hoepman, associate professor of privacy enhancing protocols and privacy by design at Radboud University

01-06-2018

There is a distinct difference between sharing threat intelligence in ISACs or trusted communities and automated sharing in the National Detection Network. It is necessary to have a clear legal framework for private organizations to participate in the NDN, and they should be transparent about their participation towards their customers.

To achieve the desired participation possibly it might be necessary to create a legal obligation for certain organizations to share events.

Data protection legislation applies to some types of threat intelligence. If IP addresses and domain names can uniquely identify natural persons, they become personally identifiable information thus fall under the General Data Protection Regulation. If an IP address or domain name belongs to an organization, it will depend on the details of the case if it is personally identifiable information.

Privacy enhancing techniques could be used for confidentiality in a threat intelligence platform, as a graduate student described in his thesis (Jongsma and Hoepman 2015).

The AbuseHUB knowledge sharing system of Dutch Internet Service Providers could function as a model for the National Detection Network. It has existed since 2014. In this system evidence of botnet infections is shared between ISP's, enabling them address infections on their networks. In addition, independent 'reliable notifiers' like SIDN Labs and the NCSC are able to share evidence of infections with ISP's (SIDN Labs 2015).

A.3.4 Marc Wijnands, Chief Security Officer at Rijksdienst voor Ondernemend Nederland (RVO)

19-06-2018

RVO is part of the Ministry of Economic Affairs of the Netherlands, but we are responsible for our own IT security. We have a security office of 8.5 FTE, which I am responsible for. I report directly to the general director of the RVO. Me and the team Security Office signal and respond to issues of information security for RVO, and promote security awareness for our organization and its employees. Throughout the organization we have representatives from various departments who report on and discuss security for their department.

Our assets include also the intellectual property in the Dutch patent office, and personal data of employees. We need to pass yearly audits in order to continue to use DigiD (identity verification by Dutch government), which we need to provide services to Dutch businesses. Threats include hacking, but also employee error.

We have compartmentalized our networks using authorizations. Technical administration of most systems happens at Dictu, a shared service organization in which parts of Dutch government have pooled their ICT management for efficiency.

All network detection measures are therefore placed at Dictu. We rely on them to notify us if they detect threats on our network. Dictu also is ISO-certificated. To this end I can imagine Dictu might want to participate in the NDN. They are free to choose their means, but we have service-level agreements.

We share knowledge with other organizations in Dutch government, like how to approach security awareness. I believe the greatest risks do not come from outside but originate in unintentional behaviour of employees (lack of awareness).

A.3.5 Sarah Brown, independent researcher

20-06-2018

At the ACM on Workshop on Information Sharing and Collaborative Security I was on the program and planning committees, and presented O. Serrano, Dandurand, and Brown 2014 and Brown, Gommers, and O. Serrano 2015.

Not all threat platforms are created equal. The threat intelligence cycle exists of the steps: collection of data, normalization, enrichment, analysis, presentation and disseminate of results. I describe the steps of the process cycle for various platorms in (Brown, Gommers, and O. Serrano 2015).

Many products focus on a specific aspect of the cycle, like collection or presentation of data. There still isn't one perfect tool that addresses all levels of the threat intel cycle perfectly, and outputs information at the right strategic, tactical, and operational levels.

There also isn't necessarily a 'best' CTI format, but I think STIX captures well what is important about threats. While it used to be hard to explain to people why STIX was important, I feel ongoing work building on it from the MITRE ATT&CK group is easier to explain. Their framework is represented in STIX and can be used to express the TTP's that are used once an attacker is inside the network. It could be used to describe types of lateral movements, conduct red-teaming exercises, and create SIEM tool rules for detection.

Threat intelligence platforms facilitate exchange of information, but they will not build trust. That really happens over a cup of coffee: you need a shared problem or experience that leads you to feel that someone can be helpful to you and your can trust them with your sensitive topic. It happens either organically like this, or you represent companies with aligned interests. This might evolve into a community, where tools can facilitate information exchange. These communities take time to develop in their own way.

When building a tool you need to have a community in mind that will make use of it: a group of people that needs something, and that can help you by offering their requirements for the problem. This is the opposite approach of 'build it, they will come'. If you have a platform, this does not mean that sharing will happen.

On the other hand, it's not necessary to have a fancy platform for sharing to happen. I've seen researchers make huge progress using tools like Skype. That is to say: if you have a will to share, it will happen.

For an existing community to move a new tool like the NDN, there needs to be a recognition that existing tools are not sufficient. There must be a clear need. Sometimes you don't need a system for sharing, but just a common format.

When you're consuming data there are a number of factors that determine the level of commitment to a CTI community. First, content. The type of data that will be there needs to be very clear for the participants. It is not enough to say you will exchange 'threat intelligence', the information should have value for a specific group or sector. Second, trust. The group should be the right size and participants should be trusted. And third, the right format. Information needs to presented at the right level, varying from an executive trend report to operational network information. The information exchanged needs to be actionable for the person receiving it.

Companies might decide to share information for reasons of reputation, as result of a legal obligation, or to show due diligence. But ideally you would be sharing to help others, and recognize that this will come back to you.

When it comes to the decision of sharing research or sightings, the factors of content and format are less important. Here trust is the most important. You want to be sure you get credit for your work. In terms of confidentiality, you need be very clear on what handling norms are.

I want to emphasize again how important it to think about the people and the process, outside of the technical platform. You can put platforms in place, people can be connected over the internet, but in order to maintain trust people have to meet face to face at for example conferences or workshops.

Ideally for such trust-building meetings, you don't invite many people. Perhaps around twenty. This is so that you can make everybody present their work or status. This works as a great icebreaker and more or less guarantees that there are no free riders. It also helps align people from the same level.

Larger bodies of people working together should be broken down into trust groups. Look for example at the FS-ISAC, with over 4000 members. They are working together on general financial cybercrime, but they organize conferences so that natural formations of smaller communities arise that can stay in touch throughout the year more intensively. Threat intelligence platforms should facilitate the large bodies as well as the smaller trust groups.

It would be a good idea if threat sharing communities could think actively on how to bring new members in. Facilitating capacity building in trust groups could be used to raise maturity for many organizations. Using this approach a goal for the NCSC in this regard could be to go one level down from only critical infrastructures, and also raise the maturity of the second-most important organizations.

A.3.6 Alexandre Dulaunoy, security researcher at CIRCL.lu

06-07-2018

MISP initially started in 2011 as platform for sharing malware samples and indicators, to address a specific usecase of a group of CSIRTs. It has now grown into a multi-purpose platform for information sharing and threat intelligence management with many contributors.

On our website we list around 6000 organizations that are now using MISP, but those are just the ones we know about. Based on the bug reports we receive, it is likely more.

We at CIRCL.lu still use and develop the tool. The core development team consists of 7 people, and there are 240 contributors to the open-source project. From these around 30 contributors are active on a daily basis. We get some funding from the European Commission for continuity of the core development team.

In our governance of the platform we also take other use-cases into account. Proposals for features or usecases are evaluated by the number and type of organizations requesting them. We try to satisfy a lot of usecases, but will not focus on edge-cases. Sometimes we include features but do not enable them by default.

We organize regular hackathons so that contributors can meet each other and work on features and integrations with other systems. We organize trainings all over the world, both to educate in the use of MISP and to collect requirements to incorporate into the roadmap.

Now that the project is growing and we have a large userbase, we want to bring more people onboard to contribute to specific aspects. We want to make the project more modular, so that many people can contribute without having to touch the core code of the project.

The modular approach would enable us to be more inclusive to non-coders as well, by allowing for example analysts to contribute to the standard.

This governance model has grown organically, and currently is fitting to the demands we face. However we are continually learing, see for example my slides on how to organically build a threat intel sharing standard. In addition, we are working on a book of best practices for CTI community building.

We want to support the type of information sharing in the National Detection Network, or within ISACs. From the NCSC-NL we receive feedback and contributions to the project, and they help us collect requirements.

The 'sightings' feature for example was included by request from the NCSC-NL for the National Detection Network, and they funded implementation. It started out as an optional feature, but it is now enabled by default and has grown into a critical feature. We will continue working on the feature in next iterations.

The way the NCSC uses multiple interconnected instances of MISP is very common and the platform is going more in that direction, especially when you want to segregate data, or are bound to technical requirements or rules. In Germany for example they have more than 60 instances. A large corporation has even built a tool on top of MISP to manage the infrastructure because they use close to 100 instances. We are in discussion with this organization to make the tool open-source.

In the future we want to extend the protocol to enable the exchange of specific elements without sharing the full dataset.

The goal of MISP was initially to collect and share data. We have seen an evolution in what people are doing with MISP, our users have gotten very creative. For example, they started exchanging complex objects with relationships, and we supported this by building an event graph view. In this way, the focus of MISP shifts from collection to analysis of data.

We have introduced support for the MITRE ATT&CK framework. We have seen that as the graphical user interface is easier, people use features more and apply standards better.

When it comes to commercial alternatives to MISP, we look at what they are doing, but since we are an open-source project we don't see them as competitors and welcome integrations. We see MISP as an ecosystem and integrate with other open-source projects like the Hive by the French central bank.

A.3.7 Geert Munnichs, coordinator technology assessment at Rathenau Institute

16-07-2018

Geert Munnichs, coordinator technology assessment at Rathenau Institute 16-07-2018

State-level actors succeed in penetrating networks while leaving minimal traces, as the must-see documentary Zero Days convincingly shows. This is corroborated by the yearly reports of the AIVD and MIVD, which tell us that the attacks we detect are just the tip of the iceberg NCSC (2015). An important question to address in your research is therefore what you detect and what you cannot detect. We must assume that China and Russia are deep in the networks of vital sectors of Western countries like the Netherlands, and that vice versa Western intelligence agencies are doing the same.

Looking from the perspective of national government, it makes sense to prioritize attention by focusing on vital sectors. Interests between government actors and vital sector organizations are very much aligned in terms of national security. But the government should look beyond vital sectors as well, and consider for example security of elections. These are the foundation for any democracy. You could argue that the (assumed) meddling by Russia in the United States Presidential elections did more damage than say, a disruption of a drinking water company would have.

The demarcation of 'vital sector organizations' is hard: where to draw the line between current vital sector organizations and other private sector organizations that might benefit from the help of the NCSC? A Digital Trust Center is now being set up to assist all non-vital private sector organizations including SME's ("MKB") with cybersecurity. The sheer breadth of this mission leaves out a group of high-tech industry organizations that might benefit from more specific expertise. From a strategic-economic perspective it seems to me unwise to let high-tech companies rely on the Digital Trust Center. Economic espionage does not have disruptive effects in the short term in the same way that sabotage of vital sectors would. But in the long term, it could undermine the national revenue model. Possibly it could be explored to make high-tech companies an additional vital sector.

The approach to security in the Netherlands using ISACs is quite advanced, as I understand. It is interesting to note that the NCSC takes an advisory, information-sharing and facilitating role in these ISACs, and does not supervise the security level of participating private organizations. In defense of this, the NCSC argues that this would endanger the trust relationship they have with the private organizations. Some believe the role of the NCSC is not active enough. In this respect, the Rathenau institute proposes to carry out a yearly hacking-test for vital sector organizations.

It is hard to estimate if the legal framework for intelligence agencies is adequate, as we're going through legal developments that will have to prove themselves in practice. The Rathenau institute has been involved in the policy consultation of the new legal powers of the Dutch intelligence and investigative agencies ("Wet op de Inlichten- en veiligheidsdiensten, resp. Wet computercriminaliteit 3"). These are necessary extensions of the powers of these governments bodies, however we point out that there should be sufficient attention paid to the legal position of the citizen and independent oversight over the application of powers. In my view, government agencies should not take a defensive stance in this discussion, but should actively plea for adequate oversight.

Cybersecurity awareness of citizens has greatly increased over the last two years, among other things as a result of the WannaCry and NotPetya ransomware campaigns. When I was writing the Rathenau report on cybersecurity challenges Munnichs, Kouw, and Kool (2017) I saw the U.S. National Security Agency as a relevant actor for domestic issues in the Netherlands: they are infamous in their capabilities to protect their interests, but had briefly before been hacked as well. I think the National Detection Network should take this reputation of government agencies for the citizen into account.

A.3.8 Richard Kerkdijk, Senior Security Consultant at TNO

25-07-2018

The interviewee was asked to respond to elements from the first iteration of the process design for the National Detection Network. The recommendations to the NCSC were in the categories technology, institutions, and process. They are printed below in italics.

Technology

1. *Establish concepts central to the system. Define for all stakeholders what is meant in context of the NDN by terms like sensors, CTI, TTPs, events, and sightings.*

   Communication of concepts should go beyond this and take the form of specifications, for concepts that the participants are expected to use. Consider design choices for the 'sighting' concept: what observables were detected? Where in the network? Was it a true positive? What was the impact? What was the response? Should the IDS or analyst timestamp be used? These are all possible attributes of a sighting, and a deliberate choice should be made about what the NCSC asks participants in the NDN to share.

For government organizations the NCSC has a certain degree of decision-power, but when it comes to collaboration with private organizations with their own infrastructure, you need to create specifications.

First the NCSC should develop a clear vision for itself on these concepts, only then should it enter into dialogue with these organizations on what they can deliver. This does not need to be all participants; a pilot project with a few organizations could result in specifications.

2. *Communicate system boundaries and roadmap. Address existing ambiguity between MISP and TIP systems. Communicating clear expectations is a precondition to achieving participant commitment.*

   Alternatively to communicating some of these what I see as internal choices for the NCSC, you could perhaps guarantee upward compatibility on the platform API. This means the API would need to be managed well, and outputs of the platform should be guaranteed.

3. *Define platform security assurance level. Which threats are to be defended against and what level of security is required. Possibly based on ISO 27001 and 27002 norms, or requirements for handling classified information by NBV.*

   Third party assurance, like independent audits of the system could be used to increase trust. This will become more important as participants start sharing more of their own intelligence.

   In addition, the responsibility of the NCSC for platform security should be bounded as participants have responsibilities here too, for example in storing the data responsibly.

4. *Explore privacy enhancing techniques. Increase trust for information sharing between semi-honest parties (i.e. private organizations) using obfuscation and anonymization, for e.g. event source or hit context.*

   This would help in increasing trust, as just discussed. A means that you should explore is secure multi-party computation.

Institutions

1. *Communicate system goals and owner mandate. Powers, responsibilities, and limitations stemming from legal framwork including Wgmc, Bir, Wiv, Avg, and Wob should be clear for all stakeholders.*

2. *Reason from social value. Organizations not currently considered 'vital sector' can be valuable targets. If current institutions (i.e. Wgmc) are limiting the constituency of the system, these should be changed.*

   My suggestion would be to explore a decentralized approach through sector-CERTs (e.g. Z-CERT) as intermediaries for non-vital sector organizations, as CERTs are considered constituency of the NCSC. The exchange of CTI between sector-CERTs and their constituents could in turn still be facilitated by the NCSC.

3. *Define confidentiality requirements for participants. Lay down social norms or legal consequences for failing to maintain TLP confidentiality norms. Explore AIVD certification procedure for handling classified information.*

   This would form assurance for mature organizations that want to share intelligence. But such requirements could also form a barrier to entry for smaller organizations. Therefore I recommend tailoring of requirements to groups of participants.

4. *Enable trust circles. Facilitate small-scale communities or collaborations in NDN technical and organizational architecture. These could be sector-based like ISACs, maturity-based, or ad-hoc. Model the cooperation in NDN after what works offline.*

   Ad-hoc communities are particularly interesting. I describe how cloud providers like HPE Threat Central and TreatConnect offer such features for temporary collaboration around a threat in Fransen and Kerkdijk 2017, table 5.2.

Process

1. *Use the process to raise maturity. Establish standards and offer capacity building programs, e.g. to help organizations set up a SOC so that it is aligned with other organizations in the NDN. Consider promoting SOC-as-a-service.*

   Helping raise maturity is already a task of the NCSC, and their existing factsheets might help in this effort.

   However, there is no one-size-fits-all solution. Capabilities do not stand by themselves, and there are preconditions before an organization can for example set up a SOC. In the same way, there are certain capabilities needed before an organization can use the intelligence derived from the NDN in a meaningful way.

2. *Fit communication to maturity level and role responsibilities. Organizations should be addressed with appropriate expectations on their role in the community, taking into account the organizational maturity and capabilities of the role of the point of contact.*

3. *Develop comparative reputational metrics to promote sharing sightings. In order to achieve collective action through sharing of sightings, the 'carrot' should be attempted before the 'stick'. Highlight leaders in the community to establish a norm of sharing (see e.g. van Eeten 2016, botnet mitigation for ISPs).*

   Vendor-based CTI platform ThreatAlliance has deliberately formulated high requirements to join their community: deliver 1000 malware samples of specific types that are not already known in VirusTotal. I give this example in Fransen and Kerkdijk 2017, figure 5.2.

   While this approach might be too strict for NDN, I feel a soft approach using reputation metrics might work as incentive to perform better.

   The design of metrics should happen carefully, as metrics should indicate community involvement, and *not* security capability.

Appendix B

STIX architecture

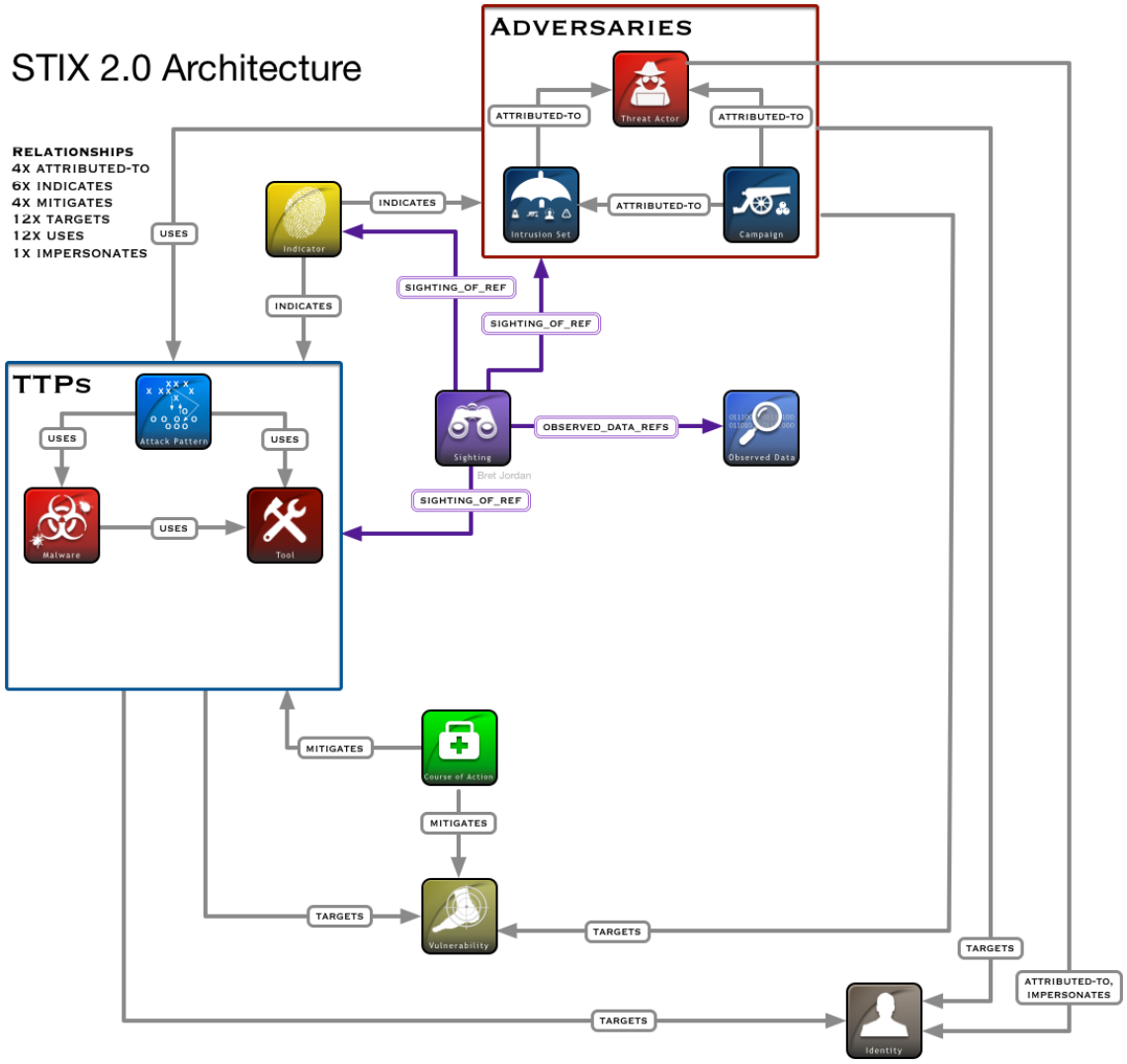

Figure B.1: STIX 2.0 architecture

More information on the STIX architecture can be found on https://oasis-open.github.io/cti-documentation/stix/. All STIX icons and figures by Bret Jordan are licensed under Creative Commons BY-SA 4.0.

Appendix C

Design validation

This overview supports the validation of the proposed process design for the National Detection Network in Section 7.3.2 using the requirements of Chapter 5, by mapping them to the process activities of Chapter 6.

- **Requirement 1** Must unite participants around a collective problem that is made explicit.

    1. Process activity 1 – Reaffirm shared goals of the system owners, from which system scope and participant entry criteria should follow.
    2. Process activity 2 – Establish concepts central to the system. Define what is meant in context of the NDN by terms like TTPs, IoCs, sightings, and situational awareness.
    3. Process activity 8 – Communicate system outer boundaries and vision. Communicating clear expectations is a precondition to achieving participant commitment.
    4. Process activity 9 – Collaboratively formulate process agreements based on lessons learned in initial trust circle, in the form of social norms to establish or rules to formalize.
    5. Process activity 10 – Introduce comparative reputational metrics to incentivize and reward engagement. Highlight leaders in the community to establish a norm of sharing.

- **Requirement 2** Should have a clear legal framework for information sharing.

    1. Process activity 1 – Reaffirm shared goals of the system owners, from which system scope and participant entry criteria should follow.
    2. Process activity 8 – Communicate system outer boundaries and vision. Communicating clear expectations is a precondition to achieving participant commitment.

- **Requirement 3** Decisions should be reached collaboratively.

    1. Process activity 2 – Establish concepts central to the system. Define what is meant in context of the NDN by terms like TTPs, IoCs, sightings, and situational awareness.
    2. Process activity 4 – Gain system owner commitment for starting an interactive decision-making process.

3. Process activity 9 – Collaboratively formulate process agreements based on lessons learned in initial trust circle, in the form of social norms to establish or rules to formalize.
4. Process activity 11 – Continuously apply learned lessons to support the creation of new trust circles.

– **Requirement 4** Must decrease the costs of sharing information.

1. Process activity 2 – Establish concepts central to the system. Define what is meant in context of the NDN by terms like TTPs, IoCs, sightings, and situational awareness.
2. Process activity 7 – Start initial trust circle by offering participants in the 'reward' quadrant of the actor analysis quick-wins.
3. Process activity 12 – Continuously evaluate if the system meets its goals.

– **Requirement 5** Should increase the individual rewards of sharing information.

1. Process activity 7 – Start initial trust circle by offering participants in the 'reward' quadrant of the actor analysis quick-wins.
2. Process activity 9 – Collaboratively formulate process agreements based on lessons learned in initial trust circle, in the form of social norms to establish or rules to formalize.
3. Process activity 10 – Introduce comparative reputational metrics to incentivize and reward engagement. Highlight leaders in the community to establish a norm of sharing.
4. Process activity 12 – Continuously evaluate if the system meets its goals.

– **Requirement 6** Large communities could be organized in nested enterprises.

1. Process activity 5 – Determine CTI capability and community engagement levels for (potential) participants.
2. Process activity 7 – Start initial trust circle by offering participants in the 'reward' quadrant of the actor analysis quick-wins.
3. Process activity 9 – Collaboratively formulate process agreements based on lessons learned in initial trust circle, in the form of social norms to establish or rules to formalize.
4. Process activity 11 – Continuously apply learned lessons to support the creation of new trust circles.