Optimising cybersecurity collaboration: an evaluation of success factors and improvement measures for network cooperation within the regional cybersecurity working group in northern Netherlands

Krijnsen, Martijn

"Optimising cybersecurity collaboration: an evaluation of success factors and improvement measures for network cooperation within the regional cybersecurity working group in northern Netherlands"

Master's thesis

Author:	Martijn Krijnsen (S3225852)
Program:	Executive master cybersecurity Leiden University
Supervisors:	1. Dr. Els de Busser, Leiden University
	2. Dr. Tommy van Steen, Leiden University

Submission date: 12 September 2024

Table of Contents

Chapter 1 Introduction

1.1 The impact of online crime

Crime is digitising. Nowadays many people in the Netherlands know someone who has become a victim of online crime. Stories about victims of phishing, bank helpdesk fraud, WhatsApp fraud or hacking are common to everyone. As early as 2020, online crime was defined by the WODC as a social problem.[1] Their survey of all recent publications concerning online crime up to 2020 showed that the nature and extent of online crime is difficult to determine. This is mainly because crimes are recorded and defined in different ways. Nonetheless, throughout the years more data concerning the victimisation and perpetration of online crime has become apparent.

The WODC study estimated that at least eight per cent of the Dutch population has fallen victim to online crime. Self-reported research (Safety Monitor 2021) by CBS shows that online crime increased by 22 per cent in the period 2012-2021, while traditional crime decreased by 43 per cent. In addition, 17% of all Dutch people said they had been victims of online crime in 2021. One in ten Dutch people has fallen victim to scams, and five percent of the population has been affected by hacking.[2] Despite the unique characteristics of online crime, such as the physical distance between perpetrator and victim, the use of technology and elusiveness of the modus operandi, the impact on the victim should not be underestimated.[3] [4] The impact of digital crime is in fact comparable to the impact of offline crime.[5] About 18% of victims suffer emotional, psychological or financial consequences. Half of the victims do not talk to others about what happened to them and only 19% report it to the police.[6]

When examining the perpetrators of online crime, a distinction can be made between those who commit offences with specific ICT knowledge and those who do so without it. [7] In 2020, both groups reported high self-reported offence rates of 10 and 12 percent, respectively, compared to the 0.02 percent of suspects registered with the police in the national cybercrime database. This large gap may be explained by the low willingness to report.[8] According to CBS, only 19 per cent of victims report online crime.[9] It could also be due to the complexity of tracking down suspects of online crime.[10] Tracing in the online world is often a lot more time-consuming and complex than in the physical world.

---

1 Beerthuizen, Maurits, Sipma, Sijke, and Van der Laan, Peter. 2020. Aard en omvang van dader- en slachtofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland. Accessed at https://repository.wodc.nl/handle/20.500.12832/253

2 Centraal Bureau voor de Statistiek. 2022. Veiligheidsmonitor 2021. Accessed at https://www.cbs.nl/-/media/_pdf/2022/09/veiligheidsmonitor.pdf.

3 Henson, Billy, Reyns, Bradford, and Fisher, Bonnie. 2016. "Cybercrime Victimization." Accessed at https://www.researchgate.net/publication/314826891_Cybercrime_Victimization..

4 Moitra, Soumyo. 2005. "Developing Policies for Cybercrime." Accessed at https://brill.com/view/journals/eccl/13/3/article-p435_5.xml.

5 Bluhm, Kimberly, Borwell, Jildau,, and Stol, Wouter. 2022. "De Slachtofferimpact van Cybercrime versus Traditionele Criminaliteit: Aanknopingspunten voor Slachtofferzorg en Preventieprioriteiten." Accessed at https://www.bjutijdschriften.nl/tijdschrift/tijdschriftveiligheid/2022/3-4/TvV-D-23-00002.

6 Centraal Bureau voor de Statistiek. 2022. Veiligheidsmonitor 2021. Accessed at https://www.cbs.nl/-/media/_pdf/2022/09/veiligheidsmonitor.pdf.

7 Rokven, Josja, Weijters, Gijs and Van der Laan, André. 2017. "Jeugddelinquentie in de Virtuele Wereld. Een Nieuw Type Daders of Nieuwe Mogelijkheden voor Traditionele Daders?" Accessed at https://repository.wodc.nl/bitstream/handle/20.500.12832/180/Cahier_2017-2_2699a_Volledige_tekst_nw2_tcm28- 250948.pdf?sequence=2&isAllowed=y.

8 Van de Weijer, Steve, Leukfeldt, Rutger, and Van der Zee, Sophie. 2020. "Reporting Cybercrime Victimization: Determinants, Motives, and Previous Experiences." Accessed at https://www.sophievanderzee.nl/wp-content/uploads/2021/01/Van-de-Weijer-et-al-2020-Reporting-cybercrime-victimization-Determinants-motives-and-previous-experiences.pdf.

9 Centraal Bureau voor de Statistiek. 2022. Veiligheidsmonitor 2021. Accessed at https://www.cbs.nl/-/media/_pdf/2022/09/veiligheidsmonitor.pdf.

10 Oerlemans, Jan-Jaap. 2020. "Cybercriminaliteit en opsporing." In Basisboek cybercriminaliteit, hoofdstuk 7. Accessed at https://jjoerlemans.files.wordpress.com/2021/11/cybercriminaliteit-en-opsporing-oerlemans-in-studieboek-cybercriminaliteit-2020.pdf.

1.1.1 The current approach by police and prosecutors

The police are one of the actors dealing with the approach of combatting online crime. However, several studies show that the police have made limited progress in fighting online crime in the period 2008-2020. Even in 2020, tackling online crime was not yet fully integrated throughout the entire police organisation.[11] [12] There is too little knowledge, capacity and ability to act among many police staff, both in intake and in investigation.[13] This knowledge gap also seems to be prevalent at the Public Prosecution Service, which leads investigations and decides whether to prosecute the suspect. In 2018, 50% of online crime reports were dismissed because there was a perception that prosecution was futile.[14] In addition to the complexity of tracking down perpetrators of online crime, the aforementioned factors significantly impact the likelihood of being caught and the willingness of victims to report incidents. This aligns with the broader observation of the police and judiciary's declining authoritative position in the security domain.[15] Powerlessness in dealing with security problems is leading to a new division of security responsibilities in which the police no longer have a monopoly on fighting crime.[16] It is therefore not surprising that the Minister of Security and Justice has stated in the Security Agenda 2015-2018 that the approach to online crime must be integrated. The minister wants to focus on integrated cooperation to increase the local resilience of citizens and businesses, where possible through preventive measures.[17]

1.1.2 Integrated cooperation as a response to a 'wicked problem'

Online crime can be deemed as a 'wicked problem'. A wicked problem is a complex problem, difficult to define, never 100% solved, a problem where every approach creates new problems, each problem is a symptom of another problem, problems with confusingly many possible causes.[18] This means that no single party can provide a solution on its own. As a result, collaboration on complex issues is increasingly considered as a necessity.[19] Cooperation between organisations allows them to share their network, expertise, information and resources.[20] Collaboration can lead to a stronger sense of shared identity as participating organizations gain a better understanding and perception of each other's interests.[21] As a result, more coordination takes place on security issues. The interaction between network partners is essential for a more complete picture of the issues and a better approach where each organisation makes its own appropriate contribution.[22] On the other side, however, this can

11 Boekhoorn, Paul. 2020. "Van intake van cybercrime naar opsporing en vervolging." Accessed at https://open.overheid.nl/repository/ronl-ab43a1df-1d25-4cbe-8d26-3c332dcee2e9/1/pdf/tk-bijlage-de-aanpak-van-cybercrime-door-regionale-eenheden-van-de-politie.pdf.

12 Jansen, Jurjen, Van Valkengoed, Thijs, Veenstra, Sander, and Stol, Wouter. 2020. "Level-Up! Kennis voor politiewerk in een digitale samenleving." Accessed at https://cybersciencecenter.nl/media/1206/2020-12-01-level-up-rapport-def.pdf.

13 Huisman, Sander, Princen, Michiel, Klerks, Pieter, and Klop, Nicolien. 2016. "Handelen naar waarheid; sterkte zwakte analyse van de opsporing." Accessed at https://www.politieacademie.nl/Documents/160608%2016-048%20Handelen%20naar%20 waarheid.pdf.

14 Boekhoorn, Paul. 2020. "Van intake van cybercrime naar opsporing en vervolging." Accessed at https://www.politieenwetenschap.nl/download/?i=7c8c6118497762a9e42ca6d3132396c4b26e79873ec5b974&p= 9a61f5ddb5c5723ad614cb1f6679578df27b890265e3b3c5n.

15 Odinot, Geralda, De Poot, Christianne, and Verhoeven, Maite. 2018. "De aard en omvang van georganiseerde cybercrime." Justitiële verkenningen 44, no. 5. Accessed at https://www.bjutijdschriften.nl/tijdschrift/justitieleverkenningen/2018/5/JV_0167-5850_2018_044_005_002/fullscreen.

16 Boutelier, Jan. 2005. "Meer dan veilig: over bestuur, bescherming en burgerschap." Accessed at https://research.vu.nl/files/2090639/Boutellieroratie.pdf.

17 Rijksoverheid. 2014. "Veiligheidsagenda 2015-2018." Accessed at https://open.overheid.nl/repository/ronl-archief-d41c768f-4601-49ad-851d-4821176b0733/1/pdf/lp-v-j-0000006384.pdf.

18 Rittel, Horst W. J., and Webber, Melvin M. 1973. "Dilemmas in a General Theory of Planning." Accessed at https://www. sympoetic.net/Managing_Complexity/complexity_files/1973%20Rittel%20and%20Webber%20Wicked%20Problems.pdf.

19 Bronstein, Laura R. 2003. "A Model for Interdisciplinary Collaboration." Accessed at https://psychrights.org/research/digest/CriticalThinkRxCites/bronstein.pdf.

20 Terpstra, Jan. 2001. "Netwerken en samenwerking bij de uitvoering van beleid." Beleidswetenschap 15, no. 2: 141-168.

21 Pröpper, Igno. 2000. "Samenwerking of autonomie in beleidsnetwerken." Accessed at https://www.slideshare.net/igno/samenwerking-of-autonomie-in-beleidsnetwerken.

22 Van Bueren, Ellen, Klijn, Erik-Hans, and Koppenjan, Joop F. M.. 2003. "Dealing with Wicked Problems in Networks: Analyzing an Environmental Debate from a Network Perspective." Accessed at https://www.researchgate.net/publication/231360506_

come at the expense of an organisation's autonomy and speed of action. The tension between cooperation and maintaining autonomy is ever-present.[23] The organizations involved in the collaboration aim for their investment of time and resources to result in a successful partnership. But what makes a collaboration successful? What are the key factors for a good collaboration? Especially when it involves regional cooperation on a 'wicked problem' like online crime. The purpose of this thesis is to find an answer to these questions. In order to do so, it is important to first a gain a deeper understanding of the term ‘online crime’.

Online crime is an umbrella term of crime where ICT plays a role in the execution of the crime. In practice, it is possible to divide this term into cybercrime and digitised crime.[24] Cybercrime is a criminal activity in which ICT is used to compromise another computer, network, or network device. Think of hacking a computer or taking down a website through a DDOS attack. In digitised crime, forms of offline crime are committed online. Examples include online scams or the distribution of criminal content. In practice, these criminal activities regularly intertwine, making it difficult to determine whether something is cybercrime or digitised crime.[25] Consider, for example, bank helpdesk fraud that can take place both online by taking over someone's computer (hacking) and over the phone by persuading someone to transfer their money to another bank account. To avoid confusion, we therefore use the umbrella term online crime.
This thesis describes how cooperation in tackling online crime is organised in the Northern Netherlands. The study examines the efficacy of collaboration within the Regional Cybersecurity Working Group Northern Netherlands.

1.2 Regional Working Group on Cybersecurity Northern Netherlands

The Regional Cyber Security Working Group North Netherlands came into existence in 2020. Its participants (municipalities, the Public Prosecutor's Office, the police and the Regional Information and Expertise Centre) reflect the operational level of the Regional Police Administrative Consultation Programme (further: RBPO). Its creation was the result of the prioritisation of cyber security in the Northern Netherlands Regional Security Policy. This document sets out policy priorities for the coming years to which the municipalities, police and prosecutors have committed. Specifically, it mentions the need for an integrated approach to online crime from prevention, disruption, victim notification and detection. The different tasks and responsibility in this approach by the different organisations should be aligned as much as possible.[26]

As a capstone for a cyber security approach, the working group chose the cyber roadmap of the Centre for Crime Prevention and Safety (CCV).[27] This cyber roadmap, designed specifically for municipalities, categorizes the approach to cybersecurity into four distinct phases: (1) maintaining a secure internal network, (2) responding to cyber incidents and crises, (3) addressing cybercrime and digitized criminal activities, and (4) managing online-induced disorder. From January 2023, the working group has been joined by a team of pioneers to boost

Dealing_with_Wicked_Problems_in_Networks_Analyzing_an_Environmental_Debate_from_a_Network_Perspective.

23 Ibid.

24 Leukfeldt, Rutger, Notte¸ Raoul, and Malsch, Marijke. 2018. "Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit." Accessed at https://repository.wodc.nl/bitstream/handle/20.500.12832/2355/2839_Volledige_Tekst_tcm28-368216.pdf?sequence=1&isAllowed=y.

25 Odinot, Geralda, De Poot, Christianne, and Verhoeven, Maite. 2018. "De aard en omvang van georganiseerde cybercrime." Justitiële verkenningen 44, no. 5. Accessed at https://www.bjutijdschriften.nl/tijdschrift/justitieleverkenningen/2018/5/JV_0167-5850_2018_044_005_002/fullscreen.

26 Regionaal Bestuurlijk Politie Overleg. 2019. Regionaal Beleidsplan Veiligheid 2020-2023. Accessed at https://www.regioburgemeesters.nl/save563/.

27 Centrum voor Criminaliteitspreventie en Veiligheid. "Cyberwegenkaart." Accessed at https://hetccv.nl/themas/cyberveiligheid/cybercrime/beleid/lokale-cyberwegenkaart/.

the 'cyber thinking'. While the working group previously spearheaded the organization of conferences, its current role is more facilitative, with a focus on supporting the network of nine pioneers (four hours a week) and a full-time cybersecurity facilitator dedicated to local cybersecurity initiatives.[28] The consequence of this professionalisation is that participants have to coordinate much more and, in the process, also become more dependent on each other. The observation within the working group is that involvement of working group members takes place at different intensities and that a network-oriented approach requires different steering. The need from practitioners is a current evidence-based analysis of network cooperation applied to current ways of working. The objective is to enhance the efficacy of combatting online crime in the Northern Netherlands.

1.3 Objective of the study

Collaborating within networks is crucial for addressing complex, "wicked" problems.[29] However, some networks fail to function effectively and end up costing society money. [30] Between these two realities lies a vast area for research—specifically, research into what makes a network successful or not. This thesis aims to explore precisely that. It presents a comprehensive analysis of the factors that contribute to successful network collaboration, drawing on an extensive review of relevant literature. This accumulated knowledge will then be applied and validated in a network cooperation in the Northern Netherlands aimed at tackling online crime. It is likely that this process will also provide new insights into regional network cooperation. This leads to the following research question:

To what extent can the current network collaboration within the Regional Cyber Security Working Group in Northern Netherlands be optimized in order to enhance the effectiveness of combatting online crime?

To address this primary question, it is necessary to break it down into the following four constituent questions.

1. What are the prerequisites for successful network cooperation?
2. How is the network cooperation of the cyber security working group organised?
3. To what extent does the current network cooperation of the cyber security working group meet the preconditions for successful network cooperation?
4. What measures can be taken to improve the network cooperation of the cybersecurity working group in the northern Netherlands?

28 Regionale Werkgroep Cyberveiligheid, Notitie voorstel programma budget en beheer werkgroep cyberveiligheid, unpublished manuscript, March 22, 2024.

29 Van Bueren, Ellen, Klijn, Erik-Hans, and Koppenjan, Joop F. M.. 2003. "Dealing with Wicked Problems in Networks: Analyzing an Environmental Debate from a Network Perspective." Accessed at https://www.researchgate.net/publication/231360506_Dealing_with_Wicked_Problems_in_Networks_Analyzing_an_Environmental_Debate_from_a_Network_Perspective.

30 Ibid.

Chapter 2 Theoretical Framework

2.1. Introduction

Tackling security has not been the sole responsibility of the police for some time now. The emergence of the concept of 'wicked problems' in the 1970s caused a boost in the number of organisations active in tackling social (in)safety.[31] Without other organisations, it is not possible to achieve your own organisational interests. Technological developments have only increased interdependence. Digitalisation means that tackling online crime requires even more parties to be involved to fight safety. This movement is not only reserved for Dutch society, but is felt worldwide.[32] Organisations work together in networks to achieve their goals. There is a multitude of networks around local security. [33] Unfortunately, these do not always work effectively. According to security networks researcher Boutelier, these networks are largely "onsystematische, ineffectieve en energie slurpende overlegvormen" (unsystematic, ineffective and energy-consuming meeting formats).[34] Fortunately, we do not have to be in the dark about how a network can function successfully. The scientific study of the factors that contribute to the success of network collaborations offers significant insight. Following an examination of the concept of a network, the thesis proceeds to investigate the various factors that contribute to the success of network collaboration, as identified in the relevant literature.

2.2 What is a network?

A network is more than a sum of actors who periodically come together to work towards achieving a common interest. In this thesis, a network is defined as:

"*Min of meer duurzame patronen van sociale relaties tussen wederzijds afhankelijke actoren die zich formeren rondom beleidsproblemen of clusters van middelen en die worden gevormd, in stand gehouden en veranderd door reeksen van spelen" [35]*

(More or less durable patterns of social relations between mutually dependent actors that form around policy problems or clusters of resources and that are formed, maintained and changed through series of games)

A network contains sustainable social contacts between actors representing different organisations/departments. These social contacts are mutually dependent on each other to successfully address certain issues. A network is fluid and always in flux; as players join and leave, in addition, players within the network can play different roles. Broadly speaking, it can be said that a successful network focuses on the relationships between actors, the existing resource classification, the interaction rules and the different perspectives of the actors.[36] When dealing with wicked problems, intensive interaction is crucial. Unlike an individual

[31] Van Steden, Ronald. 2011. *Strategieën van lokale veiligheid: een achtergrondstudie en drie reflecties*. Accessed at https://research.vu.nl/files/3004582/Strategieen%20van%20lokale%20veiligheid.pdf.
[32] De Bruijn, Hans and Ten Heuvelhof, Ernst. 2011. *Management in netwerken: Over veranderen in een multi-actorcontext*. Accessed at https://books.google.nl/books?id=Ka7KouzzBRgC&lpg=PA9&hl=nl&pg=PA147#v=onepage&q&f=false.
[33] Boutelier, Jan. 2005. *Meer dan veilig: over bestuur, bescherming en burgerschap*. Accessed at https://research.vu.nl /files/2090639/Boutellieroratie.pdf.
[34] Boutelier, Jan. 2005. Meer dan veilig: over bestuur, bescherming en burgerschap. p.7. Accessed at https://research.vu.nl/ files/2090639/Boutellieroratie.pdf. Translated by author.
[35] Klijn, Erik-Hans, Koppenjan, Joop, and Termeer, Katrien. 1993. *Van beleidsnetwerken naar netwerkmanagement: een theoretische verkenning van managementstrategieën in netwerken*. p.231. Accessed at https://ugp.rug.nl/beleidmaatschappij/article/ view/26820. Translated by author.
[36] Ibid.

organisation's approach, a network approach analyses and tackles the problem from different perspectives.[37]

2.3 Success factors in relation to steering a network

A review of the literature reveals that success factors frequently interact with one another, and the governance and configuration of the network also play a significant role. The following section will provide a more detailed examination of this topic. These success factors will be further elaborated upon in the results presented in Chapter 5, where it is explained how the respondents assess the extent to which this network collaboration meets these success factors.

In practice, three forms of network governance are distinguished: self-regulating network, leader organisation network and network administration organisation.[38] A **self-regulating network** is the simplest form. In this network, each participant is actively involved in activities from intrinsic motivation and decisions are made equally and jointly. The representation of this network is done collectively and not through one organisation. Because everyone is actively involved in this network, this network is most effective with 6 to 8 actors. In addition, there should be a high level of trust across the network. A joint high consensus on the purpose of the network ensures that members are actively involved and conflicts are minimised because everyone is motivated. In this network, the complexity of tasks is often limited and members need limited networking skills.

The second form is the **leaders' organisation** network.[39] This is a network in which one of the participants directs more on the objectives. The leader organisation is responsible for administration and facilitates the network so that network objectives can be achieved. The organisation is often also the face to formal bodies and ensures legitimacy of the network. The network can become less effective if the leader makes their own agenda dominant or takes on too many networking tasks. This can create distance between the actors and the collective network goals, as they feel less committed to the bigger picture and retreat into their own organisational goals. This form allows for an average number of members, as not all decisions need to be discussed with all network members. For effective engagement, not all members need to have confidence in the entire network, as long as there remains confidence in the organisation leader. This organisation leader is also essential in settling conflicts over network goals. The legitimacy of the organisation leader within the network is essential for effectiveness. The leader must involve everyone to get consensus to make decisions. This requires a high degree of networking competence in this form. This does lie mainly with the organisation leader and less with the members themselves. A big question is also whether the leader who is himself also involved in content can serve the network's interests more than his own.

The third model of a network is a **network administrative organisation**.[40] Unlike the other network forms, this form has an organisation attached to the network that deals only with network governance. This means that this network can consist of a large number of members. By organising steering centrally, not all members need to be involved in decision-making. For effective deployment, not all members need to have confidence in the entire network, but

[37] Van Bueren, Ellen, Klijn, Erik-Hans, and Koppenjan, Joop F. M.. 2003. "Dealing with Wicked Problems in Networks: Analyzing an Environmental Debate from a Network Perspective." Accessed at https://www.researchgate.net/publication/231360506_Dealing_with_Wicked_Problems_in_Networks_Analyzing_an_Environmental_Debate_from_a_Network_Perspective.

[38] Provan, Keith, and Kenis, Patrick. 2007. *Modes of Network Governance: Structure, Management, and Effectiveness*.. Accessed at https://academic.oup.com/jpart/article-pdf/18/2/229/2768544/mum015.pdf.

[39] Ibid.

[40] Ibid.

network members need to be able to monitor the steering organisation. In this network form, the substantive input comes from the network on a daily basis and the administrative organisation only has to steer. As a result, potential conflicts around consensus on network goals are recognised early on. Steering the network professionally and objectively requires a high degree of network competences for members of this form and is this form also suitable in case of high complexity on tasks and, for example, external accountability.

2.4 Factors influencing successful network collaboration

Much research has been done on network cooperation within the framework of social sciences. Klijn and Koppenjan laid a foundation in 1993 with their exploration of management strategies in networks which was followed by many more in-depth studies.[41] As researchers, Huxham and van Vangen have contributed to the theory of collaborative advantage and effective partnerships. Terpstra and Kouwenhoven mainly focused on research into the effectiveness of Dutch local security networks.[42] The focus of researchers Provan and Kenis is mainly on the steering of networks and how a steering model can influence the effectiveness of a network.[43] In order to develop a model or enumeration that can be utilized in empirical research, the University of Gent's study on chain and network management in healthcare was consulted. The literature review conducted by the aforementioned researchers identifies the success factors that were previously described. For a study of effectiveness, they created a model in which the factors are divided into three facets.[44] The first facet concerns factors that can be linked to the organisation of the network, the second concerns quality of interrelationships between the actors involved and the last category concerns factors that concern the influence of the context in which a network operates. These facets are further explained below.

2.4.1 Success through organisation of network

The success of the network is contingent upon the fulfilment of seven key factors. The initial factor is the manner in which the network was established, whether from the bottom up or the top down. The results of the research indicate that collaboration from bottom-up networks is of a higher quality. Top-down networks do, however, require less time for organisation. The second is clarity within the network about its objectives. Here, it is important that there is as much support as possible for the shared objectives and agreement on when they have been achieved. In networks, consensus on objectives can be hampered by individual/organisational interests. The effective use of a network requires a shared goal that is greater than one's own organisational goals. According to Provan and Kenis (2008), this requires goal consensus in the network. They call this a "*governance network";* a purposeful network consisting of three or more legitimate autonomous organisations working together to achieve not only their own goals, but also a collective goal.[45] Research shows that the shape of (and governance on) the network affects its effectiveness and product strength.[46] The third factor is a good balance between autonomy of the participants and steering from within the network. Here you have

[41] Klijn, Erik-Hans, Koppenjan, Joop, and Termeer, Katrien. 1993. *Van beleidsnetwerken naar netwerkmanagement: een theoretische verkenning van managementstrategieën in netwerken.* Accessed at https://ugp.rug.nl/beleidmaatschappij/article/view/26820.

[42] Terpstra, Jan and Kouwenhoven, Roderik. 2004. *Samenwerking en netwerken in de lokale veiligheidszorg*. Accessed at https://www.politieenwetenschap.nl/download/?i=373b7a22aae1c4b0da0d018b87445929797e2bd9d092cbb9&p=6c0e0259d410df373f634afd7b64003f51861e50f8802b0c.

[43] Provan, Keith, and Kenis, Patrick. 2007. *Modes of Network Governance: Structure, Management, and Effectiveness*.. Accessed at https://academic.oup.com/jpart/article-pdf/18/2/229/2768544/mum015.pdf.

[44] Van Tomme, Nele, Voets, Joris, and Verhoest, Koen. 2011. *Samenwerking in ketens en netwerken: praktijkervaringen uit de zorg- en welzijnssector*. Accessed at https://biblio.ugent.be/publication/5808361/file/5808363.pdf.

[45] Provan, Keith, and Kenis, Patrick. 2007. *Modes of Network Governance: Structure, Management, and Effectiveness*.. Accessed at https://academic.oup.com/jpart/article-pdf/18/2/229/2768544/mum015.pdf.

[46] Provan, Keith, and Kenis, Patrick. 2008. *Het network-governance-perspectief*. Accessed at https://pure.uvt.nl/ws/portalfiles/portal/1075353/OW_Kenis_Network_governance_Business_2008.pdf.

maximum cooperation on one side (organisations are intertwined in policy areas and steered from network) and minimum cooperation on the other side (organisations maximum autonomy and minimum steering). Risk of interdependence is a mutual dependency in a policy area. The fourth factor ties in with this; there needs to be clarity on network direction. Lack of clarity can lead to counterproductivity. Here, it is important that participants see the whole picture leading to the results within the network. Leading or facilitating the network can be done by several people. The fifth factor contributing to success is that network participants have clear roles and responsibilities towards other participants within the network. The sixth factor for success is space. Space for the network to create cooperation and innovate in the policy area, but also space for the participants from within their own organisations. If the participants are facilitated with support and mandate from their organisation, this gives a positive effect on cooperation as a whole. The final factor that contributes to a successful collaborative effort is the availability of financial resources. This may take the form of financial resources or time/capacity. An unequal distribution of financial resources among participants may impede network collaboration, potentially leading to concerns about the emergence of "profiteers" within the network. Complexity in contributing finances by participating organisations is that the benefits of a network are not equally distributed. Despite the collective realisation that individual organisations cannot solve wicked problems on their own and these should logically lead to the empowerment of social network associations, it appears that national policies, subsidies, laws, regulations and accountability systems are mainly focused on organisations rather than partnerships.[47] Organisations are judged on their own output, where the important and relevant contribution in the network is less valued.

Nr.	Success factor		Indicator success factor
1.	Network genesis		According to members, the network started bottom-up.
2.	Objectives consensus		There is agreement among members in the network on objectives.
3.	Autonomy versus direction		There is balance in members' opinions and direction from members in the network.
4.	Clarity about direction		There is clarity on network outcomes and who is directing.
5.	Clarity about own role		There is clarity about one's own role and relationship with other members of the network.
6.	Room for development		The network member is given space from their own organisation and room for new developments within the network.
7.	Access to resources (money/capacity)		Network resources (money/capacity) are contributed by the entire network

2.4.2 Success through quality of interrelationships

In a network, people from different organisation (cultures) work together, but also bring themselves into the collaboration. This also affects the success factors for good network cooperation. From the literature review by Ghent University, four factors emerge that influence the quality of network cooperation.[48] The first factor is about sufficient presence of the following relational factors: mutual respect and trust, honesty, reliability and willingness to cooperate. These factors are important because they are necessary for good interaction and information sharing. The second factor concerns having a clear view of each other's interdependence. Participants of a network start cooperating because cooperation gives them

[47] Ibid.

[48] Van Tomme, Nele, Voets, Joris, and Verhoest, Koen. 2011. *Samenwerking in ketens en netwerken: praktijkervaringen uit de zorg- en welzijnssector*. Accessed at https://biblio.ugent.be/publication/5808361/file/5808363.pdf.

something. For example, information or extra capacity. The third factor influencing collaboration is mutual language and culture. Each participant brings their own organisational culture/methods with them. The more similarities between the participants and understanding of the differences, the less chance of misunderstandings. The last factor affecting network cooperation in interrelationships is the power relations in the network. This can include the power to make decisions, or to determine how decisions are made. A power that is often unconsciously present, but can have a great effect on the network, is the power as a participant to withdraw from the network.

Nr.	Success factor		Indicator success factor
8	Presence of relational factors		There is mutual trust, respect, honesty/reliability in the network. Thereby, everyone is up to cooperation.
9	Insight into interdependence		Network members are aware that they depend on each other to achieve success on the network objectives.
10	Mutual language and culture		Network members are aware of the organisational culture, methods, they bring with them and understands those of the other members.
11	Mutual power relations		Network members have their own influence on decisions taken.

2.4.3 Success through the influence of network context

The final success factors for successful collaboration described in the Ghent University study are related to the influence of the context in which the network operates.[49] The first factor for success has to do with the history of the network. If the network or network members can build on previous similar successful collaborations, this has a positive impact (increased trust and visibility of benefits) on the network participants. The second factor that has an effect on the impact of the network is securing participant/organisation continuity in the network. Research shows that the collusion between different participants has a major impact on the network outcome. If a participant is replaced, or if a participating organisation decides to lower the priority of network activities, this can have a major impact on the success of the network. A clear long-term commitment possibly can increase trust. The third factor is the political or policy environment in which the network finds itself. If a policy area is politically charged, this can be limiting or conducive. The chances of success are increased if the topic is considered important in politics. In addition, it can help enormously if a political actor commits to an issue. Other actors are then more likely to join because of the pressure, or because they are afraid of missing an opportunity. The last factor that can help for successful network cooperation is preventing partnership fatigue. This can arise because actors are in multiple partnerships, or because there is little progress in a network due to indecision. By maintaining a unified objective and ensuring decisions are made at the right moments, this issue can be effectively resolved.

Nr.	Success factor		Indicator success factor
12	Previous history of the network		Network members have previous positive experiences with network collaborations.
13	Assurance of participants		From the members, there is long-term commitment to participation from the network.
14	Appropriate political/policy context		The goals of networking are in line with current politically relevant issues.
15	Preventing partnership fatigue		Network members feel that there is progress in the network and are not affiliated to many networks themselves.

[49] Ibid.

Chapter 3 Methodology

This chapter outlines the methodology used throughout this research project. It starts with the design of the study, explaining which research methods were applied. This is followed by an in-depth look at the choices made in the research methods. This chapter concludes with reflections on the reliability and validity of this study.

3.1 Research methods: literature review, desk research, and interviews

This study aims to answer the following question: "To what extent can the current network collaboration within the Regional Cybersecurity Working Group in Northern Netherlands be optimized in order to enhance the effectiveness of combatting online crime?" To properly answer this question, it is necessary to first identify what factors of successful network cooperation look like. These factors facilitate the identification of successful network cooperation. The subsequent phase of the study entails the examination of these identified success factors within the context of an existing network collaboration. This study employs three distinct methodological approaches.

1. A review of the literature on the factors that contribute to success.
2. Desk research on the operational aspects of the partnership.
3. Interviews to identify success factors.

3.1.1 Method 1: literature review

The literature review was the first method used and focuses on answering the first sub-question; what are the preconditions for a successful network collaborations? It concentrates on compiling an overview of factors for successful network cooperation through the use of scientific articles and other sources on network cooperation. From the collected literature, success factors are identified and categorised. This includes specifically looking at research on network collaborations around the theme of security. During the exploration, analyses of existing network collaborations (case studies) and research on what makes cooperation between people successful were sought. During the research, Google Scholar and the Leiden University Library were used. Search words used were: network cooperation, safety, success factors, collaboration, cooperation, integral cooperation, interactions, effective network cooperation. The snowball method was applied to find new relevant publications. Interview protocols were developed based on the literature review.

3.1.2 Method 2: desk research

Desk research was applied to answer the second sub-question: how is network cooperation organised in the cybersecurity working group in the Northern Netherlands? The desk research consists out of correspondence and documents tangentially related to the RBPO working group on cybersecurity. This included the use of policy documents describing how cybersecurity has been prioritised regionally. Interim evaluations, annual reports, and presentations given by working group members were also part of the desk research. Through the chair of the working group, access was also gained to mutual correspondence, if this was in the interest of answering the second sub-question. Finally, the working group's social media channel on LinkedIn was also examined to gain insight into activities and results.

3.1.3 Method 3: interviews

Interviews were conducted to answer the third and fourth sub-question: to what extent does current network cooperation in the Northern Netherlands meet the preconditions for successful network cooperation and what handles for improving network cooperation in the Northern Netherlands exist? The content and form of the interviews was determined based on the success factors collected in the literature study. Because of the required depth, qualitative research was chosen where interviews took place with two semi-structured questionnaires. One questionnaire for network participants (see appendix III) and a second written specifically for strategic-level stakeholders from RBPO organisations (see appendix IV). The choice of a semi-structured questionnaire was made because, unlike closed questions, it provides space for the respondent to give their own interpretation of the questions. At the same time, it also provides room for the interviewer to steer the conversation.

Selection of respondents
Respondents were selected on the indicators of the success factors and network set-up as emerged from the desk research. Here, a dichotomy was made between network participants and stakeholders. For the respondents who are participants in the network, the following requirements were made; they must:

1. together represent all roads of the pioneer's network,
2. consist of a diverse group of organisations
3. consist partly of working group members active in the network
4. obviously have a good understanding of the success factors in the network.

Based on the above, the following respondents were selected and interviewed (see Appendix II):

[Removed for public version]

For those respondents who are stakeholders of the network, the following requirements were imposed:

- be a member of one of the organisations from the RBPO (Municipality, Public Prosecution Office, police, RIEC North)
- work at strategic level within the organisation
- at least one must be administrative portfolio holder of the Working group Cybersecurity
- be broadly familiar with the RBPO Working group Cybersecurity

Based on the above, the following respondents were selected and interviewed (see Appendix II):

[Removed for public version]

3.2 Data processing

The interviews took place in June and July 2024. The pioneers network participants were all physically interviewed and signed an informed consent form (see Appendix V). Stakeholders were interviewed after the network participants. These interviews took place through Teams. Via email, stakeholders provided confirmation of consent for the interviews. All interviews were recorded and transcribed. The data will be deleted after completion of this assignment. The transcripts were juxtaposed in Excel, coded using open coding. This involved looking for patterns in the respondents' answers based on characteristics of the success factors. The outcome of this was elaborated in the results chapter.

3.3 Reflection on validity

Validity in a study determines whether what has been measured is what was intended to be measured. This section describes the validity of the study in terms of construct validity, content validity and internal and external validity.
Construct validity describes how well the measuring instruments used actually measure the construct they are intended to measure. Two factors may influence this. Firstly, in the case of success factors, there is a risk that certain factors overlap with each other and are therefore not entirely independent. In this study, for example, this overlap can be seen in the three success factors related to the organisation of the network: network genesis, autonomy versus direction, and room for development. If a respondent uses the same examples and ratings for several factors, the measurement becomes less precise. As a result, certain factors may be rated more positively or negatively than they should be. A better operationalization of the success factors, with more specific and accurate definitions, could have reduced this overlap and improved construct validity. Furthermore, incorporating additional validation techniques, such as factor analysis, could help identify and adjust for overlapping constructs, thereby enhancing the overall validity of the measurements. In this study, the effect remains limited because the outcome is determined on the main line 'organisation of the network'. A second factor possibly affecting construct validity is that the literature review was conducted from different perspectives to understand success factors. These perspectives include network theory, practical studies on network cooperation and security networks, and studies related to the governance perspective of networks. Integrating these various perspectives increases the completeness of understanding success factors, contributing to higher construct validity.

Content validity, which refers to the completeness and representativeness of the measured variables relative to the entire construct you are measuring was also affected in this study. The focus of the study was to measure success factors in network collaboration. This approach makes it possible to quickly identify factors that contribute to successful collaboration within a network. However, this focus ignores the fact that the ultimate success of a network is also determined by the outcomes produced by the network. As a result, the study may not cover all relevant aspects of network success and thus may not be entire valid.
Internal validity refers to the extent to which you can state with certainty that the results of a study have not been influenced by factors other than the variables studied. Several measures were taken to ensure the internal validity of this study. First, a standardized interview protocol was employed, ensuring that all respondents were asked the same questions in the same order. This consistency minimized variation in responses due to differences in question order. Second, the interview included several rating-based questions, allowing for a quantitative comparison

of responses and ensuring that the values assigned by respondents could be systematically analysed and compared.
Although the study involved a relatively small number of respondents, this group nearly represents the entire population within the pioneers network, allowing for a diverse range of perspectives on network collaboration. The variety of themes and organisations within this group ensures that the experiences with network collaboration are relevant to a broader population in similar contexts. Throughout the research, triangulation was employed, where data obtained from desk research and interviews were analysed from multiple perspectives to gain deeper insights into the nature of network collaboration.

3.4 Reliability of the research

Reliability in a study is determined by the degree of consistency, stability and reproducibility of a study. The reliability of this study was ensured by the following measures:

- A total of three-quarters of the pioneers network has been interviewed. In order to ensure a comprehensive understanding of the network, consideration has been given to the various roles and perspectives held by its members.
- Almost all relevant stakeholders were interviewed for a strategic perspective on this network cooperation. Their perspectives contribute to a fuller picture of the success factors and give additional context to the findings.
- Semi-structured questionnaire contribute to consistency of data collected. Semi-structured interviews were used in the study. This question- and topic-oriented interview technique allows the interviewer to direct the conversation, which significantly simplifies the comparability of the interviews. An advantage of this is that it promotes consistency in the data collected, which increases the reliability of the results. However, a potential disadvantage is that certain relevant knowledge of the respondent may not be covered, as the interviewer focuses on predetermined topics. To mitigate this, at the end of the interview, respondents are given the opportunity to share additional relevant information themselves
- The researcher himself is part of the network, which may have an impact on the reliability of the study. This involvement can contribute to deeper insights during the interviews, as the researcher has extensive knowledge of the network. However, it can also pose a risk, as feedback that does not align with the researcher's perspective may not be fully recognised or appreciated. This risk is mitigated to some extent, as all interviews are recorded and transcribed verbatim. In addition, the possibility of this is reduced by an intervention. The researcher uses a second reader who reads along on the results of the interviews and supervises the patterns observed in the interviews with the respondents.

Chapter 4 Desk research results

This chapter answers the question of how network cooperation is organised at the Regional Working Group on Cybersecurity. The information comes from policy documents, annual reports, presentations, websites and correspondence. The creation of the working group is described first, followed by a discussion of its direction, working methods and finances. The chapter ends with a brief resume.

4.1 Regional Working Group on Cybersecurity

The Regional Cybersecurity Working Group North Netherlands has existed since 2020. Its participants (municipalities, the Public Prosecutor's Office, the police and the Regional

Information and Expertise Centre are an operational level reflection of the Regional Police Administrative Consultation (further: RBPO). Its creation was the result of the prioritisation of cybersecurity in the Regional Security Policy of the Northern Netherlands. This document sets out policy priorities for the coming years to which the municipalities, police and prosecutors have committed themselves. In particular, the document emphasizes the necessity for a comprehensive strategy to address online criminal activities, encompassing prevention, disruption, victim notification, and detection. It is of the utmost importance that the various tasks and responsibilities of the RBPO partners are aligned as closely as possible.[50]

The RBPO Working Group on Cybersecurity is one of four administrative working groups of the RBPO, each of which is organised around a specific theme. From the RBPO, the mayors Jan Rijpstra (Smallingerland municipality) and Koen Schuiling (Groningen municipality) are ultimately responsible for cybersecurity matters. The administrative working group is tasked with two activities. Initially, it must develop a plan in collaboration with the administrative portfolio holders to address the issue. Secondly, the working group serves as a catalyst for the aforementioned theme in the northern region of the Netherlands. To maintain a direct and efficient communication channel, the portfolio holder's representative, responsible for matters pertaining to public order and safety, is an active member of the working group, facilitating regular coordination.[51] From the outset, the following organisations were involved: the municipalities of Groningen, Leeuwarden, Noordenveld, Smallingerland, and Opsterland, in addition to the organisations Public Prosecutor's Office, police, and the Regional Intelligence Crime Agency (RIEC) of North Netherlands.[52] The aforementioned organisations were subsequently incorporated into the initiative.

4.2 Strategic focus of the Working Group

At the start of the network, inventories showed that several organisations in the working group had overlap in cybersecurity activities. In addition, the urgency for the topic of cybersecurity was also recognised.[53] The administrative portfolio holders sought to create regional added value in 2020 by establishing a good structure.[54] The cyber road map developed by the Centre for Crime Prevention and Safety (CCV) became guiding in this regard.[55]
Specially developed for municipalities, this cyber roadmap divides the approach to cybersecurity into four roads: (1) maintaining a secure internal network, (2) responding to cyber incidents and crises, (3) addressing cybercrime and digitized criminal activities (target group youth, SMEs and elderly), and (4) managing online-induced disorder.[56] The urgency on the subject from the portfolio holders led to a request to the RBPO for a thematic meeting on cybersecurity that took place on 8 October 2021.[57] During this meeting, the strategic layer of municipalities, the Public Prosecutor's Office, the police, Safety Regions and the Regional Information and Expertise Centre were taken through the cyber roadmap structure for enhancing cybersecurity; in addition, based on the cyber roadmap, a draft strategic cybersecurity agenda was presented.[58] This agenda was adopted by the RBPO on 26 November

[50] Regionaal Bestuurlijk Politie Overleg. 2019. *Regionaal Beleidsplan Veiligheid 2020-2023.* Accessed at https://www.regioburgemeesters.nl/save563/.
[51] Regionale Werkgroep Cyberveiligheid, *Notitie regionaal beleidsplan eenheid Noord-Nederland: Invulling bestuurlijk portefeuillehouderschap*, unpublished manuscript, November 15, 2019.
[52] Maria Vogelzang. "RBPO-Werkgroep Cyber." Email to the Werkgroep Cyberveiligheid, September 25, 2020.
[53] Maria Vogelzang. "Notitie RBPO Cyberveiligheid." Email to the Werkgroep Cyberveiligheid, November 5, 2020
[54] Maria Vogelzang. "Terugkoppeling Startgesprek." Email to the Werkgroep Cyberveiligheid, November 13, 2020.
[55] Maria Vogelzang, "Notitie afzonderlijke thema's regionaal beleidsplan," Email to the Werkgroep Cyberveiligheid, April 9, 2020.
[56] Centrum voor Criminaliteitspreventie en Veiligheid, *Cyberwegenkaart*. Accessed at https://hetccv.nl/themas/cyberveiligheid/cybercrime/beleid/lokale-cyberwegenkaart.
[57] Regionaal Bestuurlijk Politie Overleg. *Notitie afzonderlijke thema's regionaal beleidsplan*. Unpublished manuscript. April 9, 2020.
[58] Maria Vogelzang. "Uitnodiging en Programma Themaochtend Cyberveiligheid 8 Oktober 2021." Email to the Werkgroep

2021.[59] The strategic agenda positioned the cybersecurity working group as the focal point, overseer and driver of the strategic agenda.[60] A similar awareness-raising meeting was held on 29 September 2022, aimed primarily at those implementing within RBPO organisations.[61]

4.3 From a Conference Bureau to a Network-Oriented Approach

Since September 2022, the working group has been working in a more network-oriented way. The working group is supported by pioneers linked to the various cyber paths. Pioneers driven by a shared ambition to make the Northern Netherlands cyber-secure. As a result, activities take place on all cyber roads and several networks are created. By road, this results in the following activities;

Road 1 Maintaining a secure internal network. The pioneers have set up a regional network for municipal CISOs that meets monthly, exchanges knowledge and experiences and generates attention to this topic. As a result, funding is now available from the province of Fryslân for a Cybersecurity driver and cybersecurity is also being addressed when tackling subversive crime in Drenthe.[62]

Road 2 Responding to cyber incidents and crises. The pioneers will organise a cyber exercise in 2024 in which all the security triangles of the Northern Netherlands will jointly rehearse a cyber incident with potential disorder.[63]

Road 3 Addressing cybercrime and digitized criminal activities. Pioneers in 2024 organised two knowledge-sharing sessions with a public-private network around the themes of youth and online crime and the elderly and online crime.[64] [65] The output was captured in two infographics. One knowledge-sharing session also led to a successful grant application to the CCV.[66]

Road 4 Managing online-induced disorder. One pioneer, together with the CCV, organised a meeting for members of RBPO organisations that may face online instigated disorder.[67]

Road 5 Cyber-secure events. One pioneer held a knowledge-sharing session with public and private parties on cyber-secure events in 2023. This produced an infographic of knowledge.[68]

Cyberveiligheid, September 2, 2021.

[59] Gerretzen, Jessica. "Strategische agenda." Email to the Werkgroep Cyberveiligheid, May 16, 2022.

[60] Regionale Werkgroep Cyberveiligheid. *Notitie strategische (meerjaren) agenda Cyberveiligheid RBPO-NN 2021-2023*. Unpublished manuscript. November 26, 2021.

[61] Het CCV. "Ambtenaren Noord-Nederland Weerbaarder Tegen Cybercrime na Cybercongres." September 30, 2022. Accessed at https://hetccv.nl/ambtenaren-noord-nederland-weerbaarder-tegen-cybercrime-na-cybercongres.

[62] Regionaal Bestuurlijk Politie Overleg. *Jaarverslag Regionaal Beleidsplan Veiligheid 2023*. March, 2024. Accessed at https://regioburgemeesters.nl/save859.

[63] Ibid.

[64] Werkgroep Cyberveiligheid Noord-Nederland. "Online criminaliteit onder jongeren ook in het noorden een urgent probleem." April 22, 2024. LinkedIn. Accessed at https://www.linkedin.com/feed/update/urn:li:activity:7188115011825750018.

[65] Werkgroep Cyberveiligheid Noord-Nederland. "Cyberweerbaarheid 55-plussers: 'Thee, Tablets en Taartjes'." June 27, 2024. LinkedIn. Accessed https://www.linkedin.com/posts/werkgroep-cyberveiligheid-noord-nederland_kennisdeelsessie-online-criminaliteit-en-activity-7172910454808252416-xQxV.

[66] Het CCV. "Nieuwe regioaanpakken versterken cyberweerbaarheid senioren en laaggeletterden." July 10, 2024. Accessed at https://hetccv.nl/nieuwe-regioaanpakken-versterken-cyberweerbaarheid-senioren-en-laaggeletterden.

[67] Werkgroep Cyberveiligheid Noord-Nederland. "Roadshow 'Barrièremodel Online Aangejaagde Ordeverstoringen'." LinkedIn. January 30, 2024. Accessed at https://www.linkedin.com/posts/werkgroep-cyberveiligheid-noord-nederland_de-werkgroep-cyberveiligheid-noord-nederland-activity-7158033808808710144-qoID.

[68] RIEC Noord-Nederland. "Kennisdeelsessie Afgehackt." LinkedIn. November 2023. Accessed at https://www.linkedin.com/posts/regionaal-informatie-en-expertise-centrum-noord-nederland_kennisdocument-afgehackt-2023-activity-7132757428378513408-JRPx.

The different pathways were also visualised during a presentation to the RBPO in March 2024. All the different pioneers are visible and the role of the Cybersecurity Facilitator is also marked with a square. All pioneers are attached to the regional cybersecurity working group. See figure 1 for the visual.[69]

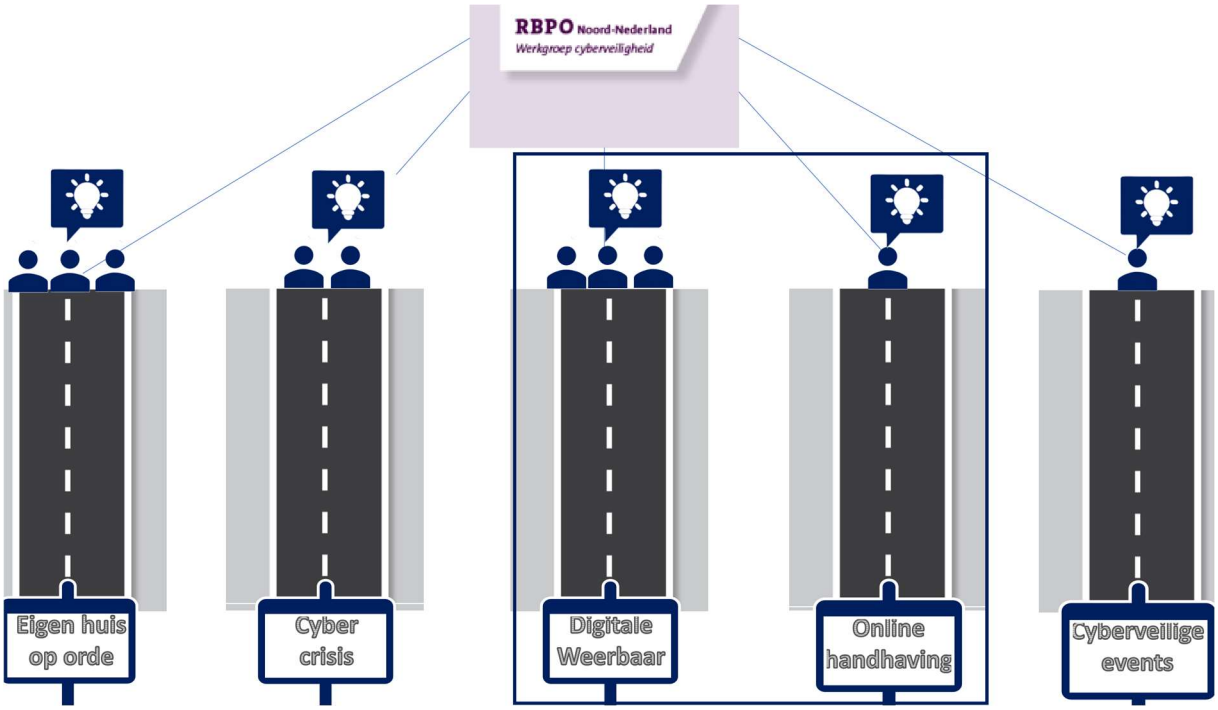

Fig. 1 Networking approach Cybersecurity working group

Since summer 2023, the working group has been reinforced with a full-time Cybersecurity facilitator. The facilitator supports the 40 municipalities in the Northern Netherlands in policy development and encourages municipalities to do activities on roads 3 and 4. They are also responsible for monthly digital online meetings where implementers working for municipalities and police in the Northern Netherlands join to increase knowledge and foster connection.[70]

4.4 Financial

The regional cybersecurity working group has a budget of €670.000 to achieve the targets in 2024-2025.[71] Of this, 630.000 euros will be contributed with incidental funds from the province of Friesland (80.000 euros), Frisian municipalities (170.000 euros), the CCV (365.000 euros) and through RBPO partners (55.000 euros). For a financial picture per road; road 1 (250.000), road 2 (30.000), road 3 (330.000), road 4 (30.000), road 5 (20.000). The financial management and formation place for the booster has been placed with RIEC North.

[69] Regionale Werkgroep Cyberveiligheid. "RBPO Presentatie Werkgroep Cyberveiligheid." Unpublished presentation, March 13, 2024.
[70] Regionaal Bestuurlijk Politie Overleg. "Jaarverslag Regionaal Beleidsplan Veiligheid 2022." March, 2023. Accessed at https://www.regioburgemeesters.nl/save789/.
[71] Regionale Werkgroep Cyberveiligheid. "Notitie voorstel Programma Budget en Beheer Werkgroep Cyberveiligheid." Unpublished manuscript, March 22, 2024.

4.5 Resume

The Northern Netherlands Regional Working Group on Cybersecurity was established in 2020 with the aim of improving cybersecurity in the Northern Netherlands. This working group falls under the strategic Regional Police Administrative Consultation and consists of tactical representatives from municipalities, the Public Prosecutor's Office, the police, and the RIEC. The focus is on strengthening cybersecurity through the five roads of the cyber roadmap. Since 2022, the working group works in a more network-oriented way, with support from pioneers who develop activities for each cyber road at regional level and who help build a relevant public-private network. The budget for 2024-2025, managed by the RIEC, is €670.000 and comes from various grants and contributions from partners.

Chapter 5 Interview results

This chapter describes the results of the interviews using the success factors from the theoretical framework. The purpose of this chapter is to answer the question whether the network cooperation meets the success factors. In addition, the interviews are also used to gain insight into handles to improve network cooperation. "The 15 success factors are divided into three main areas. Each main area is described in this chapter and concluded with a brief resume.

5.1 Success factors through organisation of the network

From the theoretical framework, 7 success factors emerge related to the organisation of the network. This section describes the presence of these factors from the respondents' perspective. These are the following success factors: network genesis, objectives consensus, autonomy versus direction, clarity on direction and own role, room for development and access to resources. This section describes the output from the interviews for each success factor.

5.1.1 Success factor 1; bottom-up network genesis

The first success factor for successful network cooperation is related to the network's genesis and working method. If there is a bottom-up genesis and working method of the cooperation, the cooperation is qualitatively better. Of the 9 respondents who are themselves active in the pioneers' network, 8 respondents consider it to be a bottom-up cooperation and 1 interviewee, respondent #I sees it as a top-down initiative and cooperation. The latter mentions that the establishment of the network comes from prioritisation by the RBPO (=top-down) and that in the collaboration, a leader group consists mainly of working group members who take the lead. This presence of a leadership group consisting of the working group members municipality of Smallingerland, Public Prosecutor's Office, police and RIEC is also mentioned by all other respondents. Several pioneers confirm the presence of a leadership group, but indicate that they see this group mainly acting in a facilitating capacity. Respondent #D indicates that the steering is mainly focused on internal coordination and progress among pioneers, but that the pioneer itself determines bottom-up what happens. One of the interviewees from this leadership group partly confirms the picture; The RBPO determines the direction and 'we discuss together with the pioneers how we are going to achieve that.' The stakeholders of the RBPO follow this line; respondent #C indicates that the intention goes top-down and that this is answered to from bottom-up approach with good ideas and appropriate implementation.

5.1.2 Success factor 2; objectives consensus in the network

The size of the second success factor depends on the degree of presence of goal consensus in a network. All respondents active in the pioneer network mention that the network's main objective is to raise awareness and resilience to cyber/online crime in the Northern Netherlands. Four interviewees specifically mentioned that cooperation is also part of the objective. Respondents were also asked about how they rate how members agree with the goals as well as the extent to which they themselves agree with them. First, a mark on how respondents think everyone agrees with the goals. Of the members, seven out of nine give at least a 7.5 for all members' assent to the goals. Of these, five graded it at least a 9.5. Respondent #D notes that the recent physical meetings have given this a huge boost. Interestingly, the two respondents who are part of the working group also give at least a 9.5. There are also respondents who give a lower mark for overall agreement from the group on the objectives. Two respondents gave a 6.8. Respondent #K indicates that this is due to a shift among some of the pioneers. As a result, a few new pioneers have stepped in to continue the work of their predecessors, but it remains

unclear to what extent they fully support the existing direction. Secondly, respondents were also asked to what extent they themselves agree with the objective. Remarkably, the respondents who earlier gave a 6.8 for their perception on the group's assent to the objectives, gave a 9 a 10 for their own assent. The average individual agreement with the objectives is notably higher, with a score of 9.5. One respondent did not give a grade, but did agree 'very much' with the objectives. Respondent #I, who earlier indicated the high top-down content of the network, joined the network later and was therefore confronted with earlier agreements (by their predecessor). Despite this respondent agreeing with the objective individually with a 10, it was stated that including new members in the objective did require more attention.

5.1.3 Success factor 3; autonomy versus direction

For the success factor autonomy versus direction, the room the pioneer network member has for input into the network plays an important role. Respondents gave at least an 8 for space to decide for themselves what they do within the network. Two members of the 'leadership group' indicated that this is mainly a question for the pioneers in the network. The pioneers interviewed feel that there is a lot of space. So much space that two respondents feel there would be no repercussions if they did nothing. One of them expressed a need for tighter control when the network is more advanced in the future. The idea behind this is to reduce confusion and uncertainty. Respondent #I gives an 8, but does not feel completely autonomous. The respondent experiences certain pressure to operate under the banner of the network, otherwise certain privileges may not be given.

The pioneers were also asked to what extent they feel like they can influence the approach of other members. Of the eight respondents who answered the question, seven indicated that they feel all room to influence other members. However, the working group members added that while they do feel they have space to influence decisions, the pioneers ultimately make the final choices. So it remains to be seen how effective this perceived space is in practice. One respondent gave a 5 for perceived space. This was because they have had little opportunity to physically discuss their direction with other members. The space to express opinions on the overall direction of the pioneer network was inquired. All but one respondent gave at least an 8 on perceived space. One respondent gave a 7 because this respondent's focus is now mainly on finding their own course. Two respondents indicated that they would like to be more involved in the overall direction of the network. One interviewee indicated a need for more dialogue on the overall direction.

5.1.4 Success factor 4/5; clarity on direction and own role

The fourth success factor “own direction” is in line with the previous success factor. Whereas the previous success factor dealt with mutual autonomy in the network, this success factor deals more with the decision line. Who makes the final decisions in the network? Six respondents indicated that final decisions are made by the working group members (Public Prosecutor's Office, police, Smallingerland municipality and RIEC) who are in the pioneers' network. However, respondents indicated that this is in consultation with the pioneers. According to respondent #I, intervention only takes place if an idea conflicts with the direction of the network. One interviewee indicated that they present their idea to a working group member to gain commitment. This is in line with respondent #G who sits in the pioneers' network on behalf of the working group. This respondent indicates that the pioneers themselves make final decisions, but coordinate with substantively strong working group members (OM and police) for confirmation on their ideas. The last two respondents also see that there is steering of the

network, but are of the opinion that the pioneer makes the final decision themselves. In close consultation with the rest of the network, though.

Clarity about one's own role and responsibility towards others also plays an important role in a successful collaboration. All respondents can give a description about the role they have. This is not to say that their role is completely clear. Respondent #A, pioneer, indicated that it is a very free role. Another respondent indicated that they were seeking more clarity on the interpretation of their role as a pioneer, as it could easily occupy their entire job. Respondent #I says that the role as pioneer is closely related to their full-time job. Another perspective is provided by the role definition of the working group members. Respondent #L says they fulfil the role of course keeper and strategy guardian. Respondent #G sees a role as a listener and practical supporter of the pioneers.

5.1.5 Success factor 6; room for development

The sixth success factor is maximised if there is room for the network to create and innovate. The facilitation of individual members by their own organisation is a key requirement here. All respondents indicated that they get all the space they need from their own organisations. Three respondents did say that the time for the network depended on the time available within their organisation. According to six respondents, it helps that their team within the organisation sees the added value of this network cooperation. This could possibly be due to overlap in objectives of their organisations and this network. Eight network members confirmed in their interviews that the network is relevant to their organisation because of its focus on cyber (7x), individual development (1x) or the organisational interest that underlines external cooperation (2x). For one respondent, these questions were not relevant because they serve as a Cybersecurity facilitator employed by the Cybersecurity working group. Two stakeholders of the RBPO indicated that they give their employees all the space they need; respondent #J indicated that they give space to theiremployee because there is energy in the network and the respondent likes to encourage this. Another stakeholder thinks a lot of space is given for this, but says they do not know.

5.1.6 Success factor 7; access to resources

Access to financial resources is the last success factor that falls under the organisation of the network. To gain deeper insight into this access, respondents were asked how they assessed the contribution of money and time within the network. Several respondents indicated that they did not know how much time others put into the network. Five respondents, three of whom were pioneers, contributed that one or more working group members invest a large amount of time. This is not borne out by the number of hours seven respondents reported investing in the network on a weekly basis. Pioneers (5x) invested an average of 3.75 hours per week against an average of 4 hours of the working group members surveyed. This may be due to the central role that working group members play in the network, making them noticeably present for everyone, unlike other members of the network. Another reason for greater time investment mentioned is the degree of coherence of the network activities in relation to the normal job. Someone who is involved in cyber full-time can be expected to have a greater time investment than someone who just does it on the side. In addition, the time investment varies. Three respondents mentioned that pioneers are especially busy around certain activities such as knowledge-sharing sessions and grant applications.

Respondents' answers are diffused around the contribution of money by network members. Their response is that the contribution of money is not brought in by one member, but also not

by all members. Several respondents have knowledge of money flows coming in, but none of the respondents who are pioneers have an overall picture. According to them, the pioneer network receives money through subsidy flows (CCV and the Province of Fryslân), but also through money contributed by the municipalities or by contributing to a product of the network as a municipality. In addition, two respondents said that the organisations' hours of work could also be seen as money. The overall picture among respondents is that the money input among members is not quite equal. Respondent #L indicates that bringing in money from grants should not be seen as the contribution of the pioneer, but as the contribution of the whole network.

5.1.7 Resume 'Success factors through organisation of the network'

This section describes the extent to which the seven success factors related to the organisation of the network are met. The first success factor (bottom-up network genesis) is partially achieved. The network originates from a top-down RBPO prioritisation, but works in practice from a bottom-up cooperation according to respondents. The second success factor (objectives consensus) is fully achieved, as there is full agreement with the objective from respondents. A critical note is that the objective was formulated very broadly, making dissensus almost impossible. The third success factor (autonomy vs direction) is also achieved, as respondents unanimously indicate that they feel they have all the space they need to decide what to do in the network. There is clarity among most respondents about direction within the network in final decisions (success factor 4). Clarity about one's own role (success factor 5) is relatively present. All respondents can describe their role, but due to lack of frameworks, some pioneers seem to be a little lost. Due to the focus on cyber, respondents get all the space from their own organisation to develop within the network (success factor 6). Access to financial resources (success factor 7) in time or money is not equal. In time, the distribution seems fairly evenly distributed among working group members and pioneers and depends on activities. The pioneers among the respondents all do not have an overall view of the money flows unlike the working group members.

5.2 Success through quality of interrelationships

Four success factors emerge from the literature that are related to the success through quality of interrelationships in the network. This section describes the presence of these factors from the respondents' perspective. These are the factors; presence relational factors, insight into interdependence, mutual language and culture and mutual power relations. This section describes the output from the interviews for each success factor.

5.2.1 Success factor 8; presence relational factors

To determine the presence of relational factors, respondents were asked about interconnectedness, approachability and trust. All respondents mentioned that honesty is very important in this network. Honesty, according to four respondents, has to do with being honest about expectations towards each other. Two respondents mentioned that in this network expectations are well-spoken. Respondent #I mentioned that within the network there is a high level of trust in each other. Respondent #Ar sees that there is trust in the network. However, the latter did emphasise that due to the limited overlap in cyber roads, there is no close cooperation. As a result, they think less trust is needed. Respondent #I is on the same page; they think the pioneers are each on an island and that they mainly exchange knowledge with each other. On interconnectedness, three groups are visible, giving an average rating of 7.5, 7 and below 5. The highest rating comes from two working group members and the Cybersecurity facilitator. This can be explained by their ubiquitous presence in the network. The second group consists of two pioneers. One of them, respondent #D indicates that they feel mostly connected to

members of the group scoring 7.5 and that they do not know some of the people in the network well. The last group scoring 5 or lower consists of three pioneers. One of them, respondent #B indicates that everyone is doing their own thing and that their topic seems far removed from the other topics. Respondent #I indicates that they joined recently and now knows some of the other members, but not all of them yet. For them, 'right now' some of the other members are not relevant. The last one, respondent #K, indicates that they are still trying to find their role and how to get as much out of the network as possible. The follow-up question on the approachability of the other network members receives a much higher score. In line with the earlier three groups mentioned, the first two groups are very close with a 10 and a 9 respectively. The third group scores a generous 8. These specifically mention benevolence (1x), helpfulness (4x) openness (3x). Respondent #I mentioned that they contacted a pioneer by phone and received an e-mail 10 minutes later with all the requested information. Respondent #A indicates that everyone is approachable, but not that everyone is visible. For them, it is not entirely clear who belongs to the network.

5.2.2 Success factor 9; insight into interdependence

The awareness that network members need each other to achieve the network goals is also present among the respondents. The working group members both say they need the pioneers to achieve the goals of the cybersecurity working group and to create movement. The pioneers interviewed say they need each other's network to strengthen their own or to get quick access to the right actors (4x). Respondent #A, for example, indicates that they have access to the right target group through this network to invite them to an event. Other dependency factors mentioned by network members are access to knowledge about cyber and certain expertise. Respondent #R indicates that they have sufficient knowledge on their specific topic, but they depend on their cyber network for a fresh perspective.

5.2.3 Success factor 10; mutual language and culture

Mutual familiarity with language and organisational culture helps network members to gain a better/deeper understanding of each other. Respondents almost all have examples of working cultures at other organisations, but have few examples of differences in culture within the pioneer network. Respondent #D indicated that in her collaboration with a network member from a private party, they get the feeling that something must always be delivered. Respondent #I indicated that during consultations, a formal character can sometimes clearly be present in the form of a fixed agenda from a member working at a municipality. Two respondents indicated that they do not see much difference in the working culture. One thinks this is because most people work from within the government; the other attributes it to the informal nature of the network. Respondent #A sees the difference in frequency of attendance as a consequence of the different working cultures; in a number of organisations (OM, police and RIEC) security is the core business, while in municipalities it is one of the core activities. The latter therefore join consultations less frequently. Respondents all appreciate the difference in working cultures. This way, they can get to know new parties, learn from others and thus make each other stronger and sharper.

5.2.4 Success factor 11; mutual power relations

The mutual power relations in the network also play an important role in successful network collaborations. Here, it can be assumed that the more sense of space and influence in the network, the greater the chances of success. Seven out of nine respondents all feel the space to influence the direction of others in the network. The same number of people also feel freedom to influence the direction of the network itself. They rate this an 8. There is however a perceived

difference in influencing and actually making decisions. Six respondents indicated that, when making final decisions, they look mainly to the working group members in the network. However, it is not clear from the answers whether this situation has already occurred. In addition, respondent #F puts decision-making within the network into perspective, as a network cannot make decisions for standing organisations. Respondents were also asked in terms of content where they think they have influence. On this, 5 pioneers interviewed indicated that they decide for themselves how to fill in the pioneer role. One pioneer stressed that the limited time commitment per week prevented them from having more influence. Another perspective came from respondent #I. They indicated that the direction is very broad, but is broadly determined by the RBPO. This gives him an autonomous position as his organisation is not under the RBPO. Respondent #G indicates that the RBPO has little influence on the interpretation of the priorities and that the network is therefore free to determine the interpretation. The two working group members indicate that they have influence on the direction of the network, but that they have little influence on how the pioneers fill it in. In this regard, respondent #L thinks it would be good to involve the pioneers more in the direction, so that it does not depend on a small group.

5.2.5 Resume 'Success factors through quality of interrelationships'

This section describes the extent to which the four success factors related to the quality of interrelationships in the network are met. First, it appears that relational factors are present in the network (success factor 8), but that there is room for growth. Interconnectedness seems to be limited by the fact that some pioneers do not yet know each other well. The high mark given by respondents for mutual approachability provides a good starting point for further growth. There is an awareness within the network that members need each other (success factor 9) for knowledge/expertise on cyber or access to people in the network. There seems to be little difference in mutual language and culture within the network (success factor 10). There is appreciation from respondents for difference in language and culture. Despite several pioneers looking at the working group members when making a final decision, it does not appear from the responses that this has happened before. Respondents experience all the space within the network to decide what to do. Because of the above, the mutual power relations seem to be in balance. In broad terms, the RBPO sets the overall direction, while in practice, the pioneer makes the decisions regarding their specific topic. The balance in practice lies in the working group members executing the RBPO's course, who cannot do so without the pioneers, and the pioneers who need the working group members to achieve their objectives

5.3 Success through the influence of network context

Four success factors emerge from the literature that have to do with the influence of the context of the network. This section describes the presence of these factors from the respondents' perspective. These are the following success factors: previous history of the network, assurance of participants, appropriate policy/political context, preventing partnership fatigue. This section describes the output from the interviews for each success factor.

5.3.1 Success factor 12; previous history of the network

Previous history with other networks has a lot of influence on the perception of network cooperation. Of course, it goes without saying that a positive previous history increases the likelihood of successful cooperation. Of the nine respondents, six had positive experiences of network cooperation and were able to name benefits of network cooperation. Respondent #D especially mentioned the importance of meeting physically to prevent it from bleeding to death. The three remaining respondents have both positive and negative experiences. Therefore, for

example, respondent #A only steps into a network that 'really' works, for respondent #L it only makes sense if you have something to work on together, so that it does not become an 'abstract talking shop', and respondent #E prefers to step into 'free' networks that are free of political considerations as much as possible.

5.3.2 Success factor 13; assurance of participants

The long-term retention of participants in the network is also a key success factor for network cooperation. To address this, members were asked how they have secured their position within their organization and to what extent they plan to remain active in the network next year. Although the immediate colleagues of all respondents are aware of the network's existence, this does not necessarily guarantee their continued involvement. Five respondents indicated that they had not yet secured this network in their organisation. Two respondents representing an organisation not covered by the RBPO did coordinate their attendance with the manager, but not on an hourly basis. Respondents' attendance thus seems to take place mainly from intrinsic motivation. This motivation is also reflected in the respondents' answer to the question whether they will still be part of the networks next year. On a five-point scale of none-certain, seven respondents indicated that they were likely or certain to remain affiliated next year. Two bet on neutral, with one respondent indicating they will stay if things continue as they are. The other lets attendance determine how the RIEC will take up a director's role on this topic. Two stakeholders say they have secured their presence, while the third is unaware of this.

5.3.3 Success factor 14; appropriate policy/political context

A network's chances of success are increased if the network's theme returns to the political agenda. All respondents from the pioneers network as the stakeholders believe that cybersecurity is on the political agenda. Besides the working group named as a result of high prioritisation by the RBPO, other examples are also given; that cybersecurity is a priority at several national organisations, the introduction of the NIS2, the many parliamentary questions around this topic, because of the large media attention to the topic, because our Council has prioritised digital security. Respondent #L also indicated that apart from the substantive political relevance, there is now also an awareness that network cooperation is the only way we can tackle complex social issues.

5.3.4 Success factor 15; prevention of partnership fatigue

The last success factor is mainly about preventing network fatigue. How to ensure that people stay actively involved in the network. For this, it is important that members feel the network delivers results. Respondents were asked about the added value of the network and how it differs from other networks. According to three respondents, what distinguishes this network from other networks is its external focus. Respondent #B indicated the formal basis in the RBPO as an added value of the network. Other respondents mentioned as added value the dynamics and freedom in the network, the possibility to make a practical contribution, the structure and the purpose and action orientation of the network. As a mark, seven respondents gave an 8 for the added value of this network. Respondent #I gave a 6.5 and mentioned that pioneers are 'colouring and dragging' in different places and have support throughout the network. In doing so, they specifically emphasize the importance of continually recalibrating.

5.3.5 Resume ‘Success through the influence of network context’

This section describes the extent to which the four success factors related to the influence of network context are met. All respondents see the importance of network collaboration from

previous network collaborations (success factor 12). Negative experiences have not changed this understanding, but have helped to better choose which networks are relevant. The safeguarding of participants (success factor 13) was not established in hours. The majority of participants have not secured their presence in this particular network in their own organisation. This means that the securing of the network is mainly based on the participant's intrinsic motivation. Despite the vast majority indicating that there is a high probability that they will still be affiliated next year, this does represent a continuity risk for the network. Whether the network's theme is relevant within a political and policy context (success factor 14) is not an issue. From all sides, this theme appears to be high-priority. The last factor is about preventing network fatigue, as members feel the network delivers results. All respondents give a positive rating on the added value of this network.

Chapter 6 Conclusions and discussion

6.1 Conclusion and recommendations

This study has examined how current network cooperation within the Regional Working Group on Cybersecurity could be professionalised to tackle online crime more effectively. The theoretical framework focused on identifying key preconditions for successful cooperation, with 15 success factors emerging from the literature. These factors were clustered into three main areas: the organisation of the network, the quality of the relationships between them, and the influence of the context of the network. The success factors were examined and asked out in the interviews to the participants of the pioneer network. It also included stakeholders' perspectives on the network cooperation. The desk research and interviews led to new insights on the quality of this network cooperation. The following findings were observed from the three main areas;

Success through the organisation of the network

Overall, most of the success factors related to the organisation of the network are reasonably to fully met. However, there are some areas of concern, such as the partial top-down approach, the broad formulation of the objective, uncertainties about the role of some members, and uneven access to, or understanding of, financial resources. These findings indicate a mainly positive collaboration, but also highlight the need for more clarity and transparency in certain aspects of this network collaboration.

Success through quality of interrelationships

The quality of mutual relations in the network is generally assessed as positive, with a good basis for further development. There is awareness of interdependence and appreciation of other working cultures, which strengthens cooperation. However, there are still opportunities for improvement, especially in promoting mutual awareness that makes it easier to strengthen mutual cooperation and connection. The equal power relations within the network seem well secured, contributing to healthy cooperation.

Success through influence of network context

The influence of the context of the network appears to be generally positive. Awareness of the need for cooperation is present, and in addition there is a high political and policy relevance of the topic and the network is positively appreciated by member organisations. However, the embedding of participants in the organisation is a weak point, posing a potential risk for the continuity of the network. The network seems to benefit from intrinsic motivation and the high priority of the topic, but could improve by creating formal structures for securing participants' involvement.

6.2 Discussion

Despite most success factors being reasonably to fully realised, there are still areas for improvement. Specifically, the partial top-down approach, broadly formulated objectives, and lack of clarity around role allocation and financial resources are highlighted. These factors underline the need for more structured and clear processes. A key issue here is how the network can provide more transparency and clarity without limiting flexibility and autonomy, which are currently perceived as positive.

The results indicate a significant degree of autonomy perceived by members, which contributes positively to their involvement and the quality of cooperation. An interesting issue for further discussion is the balance between autonomy and steering within the network; how to steer the network effectively, without limiting members' autonomy too much. This could be further explored by, for example, examining other regional networks that deal with cybersecurity and are linked to governance.

This analysis highlights that participants' commitment depends largely on intrinsic motivation. This poses a risk to the continuity of the network. A key question here is how to mitigate this risk. Can the network implement formal structures and agreements without disrupting informal, motivation-based dynamics? This could be achieved through clear role descriptions, expectations, and responsibilities.

6.3 Restrictions

A limitation may arise in this study due to the small sample size and the focus on one specific region. This limits the generalisability of the findings. In addition, the use of mainly qualitative data is a limitation, as perceptions and opinions can be subjective. These limitations could be overcome in a follow-up study by conducting a broader sample (possibly on multiple cases) and using qualitative research methods.

The continuous professionalisation of network cooperation is essential for tackling societal 'wicked problems' that are too complex for individual organisations to solve alone. Only through joint efforts and shared expertise can we achieve sustainable and effective solutions. When network cooperation is necessary, let us strive for excellence. In the words of Lord Chesterfield:

"If a thing is worth doing, it is worth doing well." [72]

[72] Stanhope, Philip D., *Letters to His Son, 1746–47*, vol. 2 (London: Ernest Benn Ltd., 1927), 303, letter dated October 9, 1746, accessed at https://www.gutenberg.org/ebooks/3351.

APPENDIX I Bibliography

The following bibliography contains all the sources consulted for this study. The list includes both primary and secondary sources, ranging from scientific articles and books to official reports and policy documents. The sources were selected based on their relevance to the research question and are arranged in alphabetical order.

1. Beerthuizen, Maurits, Sipma, Sijke, and Van der Laan, Peter. 2020. *Aard en omvang van dader- en slachtofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland*. Accessed at https://repository.wodc.nl/handle/20.500.12832/253.

2. Bluhm, Kimberly, Borwell, Jildau, and Stol, Wouter. 2022. *De Slachtofferimpact van Cybercrime versus Traditionele Criminaliteit: Aanknopingspunten voor Slachtofferzorg en Preventieprioriteiten*. Accessed at https://www.bjutijdschriften.nl/tijdschrift/ tijdschriftveiligheid /2022/3-4/TvV-D-23-00002.

3. Boekhoorn, Paul. 2020. *Van intake van cybercrime naar opsporing en vervolging*. Accessed at https://open.overheid.nl/repository/ronl-ab43a1df-1d25-4cbe-8d26-3c332dcee2e9/1/pdf/tk-bijlage-de-aanpak-van-cybercrime-door-regionale-eenheden-van-de-politie.pdf.

4. Boekhoorn, Paul. 2020. *Van intake van cybercrime naar opsporing en vervolging*. Accessed at https://www.politieenwetenschap.nl/download/?i=7c8c6118497762a9e42ca6d3132396c4b26e79873ec5b974&p=9a61f5ddb5c5723ad614cb1f6679578df27b890265e3b3c5n

5. Boutelier, Jan. 2005. *Meer dan veilig: over bestuur, bescherming en burgerschap*. Accessed at https://research.vu.nl/files/2090639/Boutellieroratie.pdf

6. Bronstein, Laura R. 2003. *A Model for Interdisciplinary Collaboration*. Accessed at https://psychrights.org/research/digest/CriticalThinkRxCites/bronstein.pdf.

7. Centraal Bureau voor de Statistiek. 2022. *Veiligheidsmonitor 2021*. Accessed at https://www.cbs.nl/-/media/_pdf/2022/09/veiligheidsmonitor.pdf

8. Centrum voor Criminaliteitspreventie en Veiligheid. *Cyberwegenkaart*. Accessed at https://hetccv.nl/themas/cyberveiligheid/cybercrime/beleid/lokale-cyberwegenkaart/

9. De Bruijn, Hans and Ten Heuvelhof, Ernst. 2011. *Management in netwerken: Over veranderen in een multi-actorcontext*. Accessed at https://books.google.nl/books?id= Ka7KouzzBRgC&lpg= PA9&hl=nl&pg=PA147#v=onepage&q&f=false

10. Gerretzen, Jessica. "Strategische agenda." Email to the Werkgroep Cyberveiligheid, May 16, 2022.

11. Henson, Billy, Reyns, Bradford, and Fisher, Bonnie. 2016. *"Cybercrime Victimization."* Accessed at https://www.researchgate.net/publication/314826891_Cybercrime_ Victimization

12. Het CCV. 2022. *"Ambtenaren Noord-Nederland Weerbaarder Tegen Cybercrime na Cybercongres."* September 30, 2022. Accessed at https://hetccv.nl/ambtenaren-noord-nederland-weerbaarder-tegen-cybercrime-na-cybercongres

13. Het CCV. 2024. *"Nieuwe regioaanpakken versterken cyberweerbaarheid senioren en laaggeletterden."* July 10, 2024. Accessed at https://hetccv.nl/nieuwe-regioaanpakken-versterken-cyberweerbaarheid-senioren-en-laaggeletterden

14. Huisman, Sander, Princen, Michiel, Klerks, Pieter, and Klop, Nicolien. 2016. *Handelen naar waarheid; sterkte zwakte analyse van de opsporing*. Accessed at https://www.politieacademie.nl/Documents/160608%2016-048%20Handelen%20naar%20waarheid.pdf

15. Jansen, Jurjen, Van Valkengoed, Thijs, Veenstra, Sander, and Stol, Wouter. 2020. *Level-Up! Kennis voor politiewerk in een digitale samenleving*. Accessed at https://cybersciencecenter.nl/media/1206/2020-12-01-level-up-rapport-def.pdf

16. Klijn, Erik-Hans, Koppenjan, Joop, and Termeer, Katrien. 1993. *Van beleidsnetwerken naar netwerkmanagement: een theoretische verkenning van managementstrategieën in netwerken*. Accessed at https://ugp.rug.nl/beleidmaatschappij/article/view/26820

17. Klijn, Erik-Hans, Koppenjan, Joop, and Termeer, Katrien. 1993. *Van beleidsnetwerken naar netwerkmanagement: een theoretische verkenning van managementstrategieën in netwerken*. Accessed at https://ugp.rug.nl/beleidmaatschappij/article/view/26820

18. Leukfeldt, Rutger, Notte, Raoul, and Malsch, Marijke. 2018. *Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit*. Accessed at https://repository.wodc.nl/bitstream/handle/20.500.12832/2355/2839_Volledige_Tekst_tcm28-368216.pdf?sequence=1&isAllowed=y

19. Moitra, Soumyo. 2005. *"Developing Policies for Cybercrime."* Accessed at https://brill.com/view/journals/eccl/13/3/article-p435_5.xml

20. Odinot, Geralda, De Poot, Christianne, and Verhoeven, Maite. 2018. *De aard en omvang van georganiseerde cybercrime*. Justitiële verkenningen 44, no. 5. Accessed at https://www.bjutijdschriften.nl/tijdschrift/justitieleverkenningen/2018/5/JV_0167-5850_2018_044_005_002/fullscreen

21. Odinot, Geralda, De Poot, Christianne, and Verhoeven, Maite. 2018. *De aard en omvang van georganiseerde cybercrime*. Justitiële verkenningen 44, no. 5. Accessed at https://www.bjutijdschriften.nl/tijdschrift/justitieleverkenningen/2018/5/JV_0167-5850_2018_044_005_002/fullscreen

22. Oerlemans, Jan-Jaap. 2020. *"Cybercriminaliteit en opsporing."* In Basisboek cybercriminaliteit, hoofdstuk 7. Accessed at https://jjoerlemans.files.wordpress.com/2021/11/cybercriminaliteit-en-opsporing-oerlemans-in-studieboek-cybercriminaliteit-2020.pdf

23. Provan, Keith, and Kenis, Patrick. 2007. *Modes of Network Governance: Structure, Management, and Effectiveness*. Accessed at https://academic.oup.com/jpart/article-pdf/18/2/229/2768544/ mum015.pdf

24. Provan, Keith, and Kenis, Patrick. 2008. *Het network-governance-perspectief*. Accessed at https://pure.uvt.nl/ws/portalfiles/portal/1075353/OW_Kenis_Network_governance_Business_2008.pdf

25. Regionaal Bestuurlijk Politie Overleg. 2019. *Regionaal Beleidsplan Veiligheid 2020-2023*. Accessed at https://www.regioburgemeesters.nl/save563/

26. Regionaal Bestuurlijk Politie Overleg. 2024. *Jaarverslag Regionaal Beleidsplan Veiligheid 2023*. March, 2024. Accessed at https://regioburgemeesters.nl/save859

27. Regionaal Bestuurlijk Politie Overleg. 2023. *Jaarverslag Regionaal Beleidsplan Veiligheid 2022*. March, 2023. Accessed at https://www.regioburgemeesters.nl/save789

28. Regionale Werkgroep Cyberveiligheid. 2019. *Notitie regionaal beleidsplan eenheid Noord-Nederland: Invulling bestuurlijk portefeuillehouderschap*. Unpublished manuscript, November 15, 2019.

29. Regionale Werkgroep Cyberveiligheid. 2021. *Notitie strategische (meerjaren) agenda Cyberveiligheid RBPO-NN 2021-2023*. Unpublished manuscript, November 26, 2021.

30. Regionale Werkgroep Cyberveiligheid. 2024. *Notitie voorstel Programma Budget en Beheer Werkgroep Cyberveiligheid*. Unpublished manuscript, March 22, 2024.

31. Regionale Werkgroep Cyberveiligheid. 2024. *RBPO Presentatie Werkgroep Cyberveiligheid*. Unpublished presentation, March 13, 2024.

32. RIEC Noord-Nederland. 2023. *"Kennisdeelsessie Afgehackt."* LinkedIn, November 2023. Accessed at https://www.linkedin.com/posts/regionaal-informatie-en-expertise-centrum-noord-nederland_kennisdocument-afgehackt-2023-activity-7132757428378513408-JRPx

33. Rijksoverheid. 2014. *Veiligheidsagenda 2015-2018*. Accessed at https://open.overheid.nl/ repository/ronl-archief-d41c768f-4601-49ad-851d-4821176b0733/1/pdf/lp-v-j-0000006384.pdf

34. Rokven, Josja, Weijters, Gijs, and Van der Laan, André. 2017. *Jeugddelinquentie in de Virtuele Wereld. Een Nieuw Type Daders of Nieuwe Mogelijkheden voor Traditionele Daders?* Accessed at https://repository.wodc.nl/bitstream/handle/20.500.12832/180/ Cahier_2017-2_2699a_Volledige_tekst_nw2_tcm28-250948.pdf?sequence=2&is Allowed=y

35. Stanhope, Philip D., *Letters to His Son, 1746–47*, vol. 2 (London: Ernest Benn Ltd., 1927), 303, Accesed at https://www.gutenberg.org/ebooks/ 3351.

36. Tasler, Nick. 2014. *"How to Avoid Collaboration Fatigue."* Harvard Business Review, July 10, 2014. Accessed at https://hbr.org/2014/07/how-to-avoid-collaboration-fatigue

37. Terpstra, Jan. 2001. *"Netwerken en samenwerking bij de uitvoering van beleid."* Beleidswetenschap 15, no. 2: 141-168.

38. Terpstra, Jan, and Kouwenhoven, Roderik. 2004. *Samenwerking en netwerken in de lokale veiligheidszorg*. Accessed at https://www.politieenwetenschap.nl/download/?i=373b7a22 aae1c4b0da0d018b87445929797e2bd9d092cbb9&p=6c0e0259d410df373f634afd7b64 003f51861e50f8802b0c

39. Van Bueren, Ellen, Klijn, Erik-Hans, and Koppenjan, Joop F. M. 2003. *Dealing with Wicked Problems in Networks: Analyzing an Environmental Debate from a Network Perspective*. Accessed at https://www.researchgate.net/publication/231360506_ Dealing_with_Wicked_Problems_in _ Networks_Analyzing_an_Environmental _ Debate_from _a_Network_Perspective

40. Van der Laan, André, and Hesseling, René. 2021. *"Cybercriminaliteit door Nederlandse Jongeren."* CCV Secundant, August 16. Accessed at https://ccv-secondant.nl/platform/article/cyber criminaliteit-door-nederlandse-jongeren-1

41. Van de Weijer, Steve, Leukfeldt, Rutger, and Van der Zee, Sophie. 2020. *"Reporting Cybercrime Victimization: Determinants, Motives, and Previous Experiences."* Accessed at https://www.sophievanderzee.nl/wp-content/uploads/2021/01/Van-de-Weijer-et-al-2020-Reporting-cybercrime-victimization-Determinants-motives-and-previous-experiences.pdf

42. Van Steden, Ronald. 2011. *Strategieën van lokale veiligheid: een achtergrondstudie en drie reflecties*. Accessed at https://research.vu.nl/files/3004582/Strategieen%20van%20 lokale%20 veiligheid.pdf

43. Van Tomme, Nele, Voets, Joris, and Verhoest, Koen. 2011. *Samenwerking in ketens en netwerken: praktijkervaringen uit de zorg- en welzijnssector*. Accessed at https://biblio.ugent.be/publication/5808361/file/5808363.pdf

44. Vogelzang, Maria. *"Notitie RBPO Cyberveiligheid."* Email to the Werkgroep Cyberveiligheid, November 5, 2020.

45. Vogelzang, Maria. *"Notitie afzonderlijke thema's regionaal beleidsplan."* Email to the Werkgroep Cyberveiligheid, April 9, 2020.

46. Vogelzang, Maria. *"RBPO-Werkgroep Cyber."* Email to the Werkgroep Cyberveiligheid, September 25, 2020.

47. Vogelzang, Maria. *"Terugkoppeling Startgesprek."* Email to the Werkgroep Cyberveiligheid, November 13, 2020.

48. Werkgroep Cyberveiligheid Noord-Nederland. 2024. *"Cyberweerbaarheid 55-plussers: 'Thee, Tablets en Taartjes'."* LinkedIn, June 27, 2024. Accessed at https://www. linkedin.com/posts/ werkgroep-cyberveiligheid-noord-nederland_kennisdeelsessie-online-criminaliteit-en-activity-7172910454808252416-xQxV

49. Werkgroep Cyberveiligheid Noord-Nederland. 2024. *"Online criminaliteit onder jongeren ook in het noorden een urgent probleem."* LinkedIn, April 22, 2024. Accessed at https://www.linkedin.com/feed/update/urn:li:activity:7188115011825750018

50. Werkgroep Cyberveiligheid Noord-Nederland. 2024. *"Roadshow 'Barrièremodel Online Aangejaagde Ordeverstoringen'."* LinkedIn, January 30, 2024. Accessed at https://www.linkedin.com/posts/werkgroep-cyberveiligheid-noord-nederland_de-werkgroep-cyberveiligheid-noord-nederland-activity-7158033808808710144-qoID

APPENDIX II Respondents

[Removed for public version]

APPENDIX III Interview protocol member network

First of all, thank you for participating in this research. This research provides more insight into how, based on success factors of, network cooperation can be professionalised. For this purpose, the success factors, known from the literature, are placed on a network collaboration. In this case, that is the network of pioneerss' network that falls under the RBPO Working Group on Cybersecurity in the Northern Netherlands.

You are being interviewed because you are involved in the pioneers network. In this interview, you will have the opportunity to give your views on the presence of these success factors and how they could possibly be professionalised. You will also be given the space to indicate what, for you, are important success factors of network cooperation. This will help expand knowledge about success factors.

Important!
- In principle, all input is processed anonymously in a final report. This is also described in the consent form. How would you like to be mentioned in the appendix of this study where the list of respondents is; name/function, position or organisation?
- This interview will be worked out verbatim. Would you still like to receive this for verification?
- This survey will be recorded and then edited verbatim. The recording will be deleted immediately afterwards and the anonymous verbatim recording will be kept and can be used to verify the reliability of the research within the university. Do you consent to a recording?
- Get a consent form signed
- Any further questions?

Start interview

1. How long have you been involved in the pioneers network?
2. On average, how many hours per week do you spend on the pioneers network?
3. What roles can you distinguish in the pioneers network?
4. Describe your own role within the pioneers network.

A. Questions part 1 'success through organisation of network'

A1 How would you describe the steering form of the network?
   a. Self-managing (network determines its own direction)
   b. Leader organisation (one organisation leads the network)
   c. Network administrative organisation (organisation formally set up to lead the network)

A2 What do you think are the objectives of the pioneers network?

A3 To what extent do members of the pioneers network agree with these objectives?

0 = no one agrees
10 = everyone agrees

A4 To what extent do you personally agree with these objectives? How do you think they could be improved?

A5 What are your own objectives in the network?

A6 Do you see the pioneers network as a bottom-up or a top-down initiative? Please explain!

bottom up = employees work collectively to identify problems without being mandated by a leader or policy
top-down = employees are activated/guided by decisions or directions made by leaders at the top of their organisation.

A7 What space do you experience within the pioneers network to be able to decide for yourself what to do? How do you think this could be improved?

0 = I cannot decide anything myself
10 = I decide everything myself

A8 What space do you experience within the pioneers network to give your opinion on the direction of the network? How could this be improved?

0 = No space
10 = All space

A9 What space do you experience within the pioneers network to influence the approach/methods of others? How could this be improved?

0 = No space
10 = All space

A10 Who within the pioneers network do you see as the ones who make final decisions take? Explain!

A11 How much space do you get from your own organisation to join this network?

A12 Please rate the TIME investment in the pioneers network? How do you think it could be improved?

0 = Everyone contributes the same amount of time

10 = The time investment is mainly done by one member

A13 Please rate the MONEY investment in the pioneers network? How do you think it could be improved?

0 = Everyone contributes the same amount of money
10 = The money investment is mainly done by one member

A14 Do you feel the network is producing results that add value? If so, cite examples. How do you think it could do better?

B. Questions Part 2: 'Questions around success through quality interrelationships'

B1 How would you describe the mutual trust in the network? Are there examples that you could use to describe it? How do you think it could be improved?

B2 Are there differences of opinion within the network about the approach?

B3 If yes, how are different disagreements or views within the network dealt with? Do you have any examples? How do you think it could be done better?

B4 How important is honesty in this network?

B5 How important is trustworthiness in the network?

B6 Rate the extent to which you need others in the network to achieve your own goals. Do you have any examples?

0 = I do not need the other network members

10 = I need the other network members to achieve my own goals

B7 To what extent do you also see different working cultures within the network?

B8 How do you notice this in a the collaboration with others? Do you have any examples?

B9 How do you value the different working cultures within the network?

B10 How connected do you feel to other network members? Explain!

0 = no connection

10= maximally connected

B11 How approachable do you find the other network members? Explain!

0 = not approachable

10= very approachable

B12 Describe where you have influence within the network (deepening question on which decisions do or do not you have influence?) How do you think things could be better?

C. Questions part 3 'success through context of network'

C1 What are your previous experiences with network collaborations? (in-depth question; how do you value these collaborations)

C2 How likely do you think it is that you will still be a member of this network next year? Explain!

No chance small chance neutral big chance for sure

C3 How have you secured your affiliation/time commitment to the network within your own organisation?

C4 How is the added value of this network assessed from within your own organisation?

C5 To what extent do the objectives of this network align with the objectives from within your own organisation? How do you think they could be better?

C6 Do you think the objectives of the network are in line with current politically relevant issues? Please explain!

C7 To what extent is this network different from other networks you are a member of? Please explain!

General questions

1. Rate the added value of the network cooperation created by the pioneers network and explain why.

   0 = no added value

   10 = maximum added value

2. What do you yourself think is an important factor that determines whether a network collaboration is successful?

3. How could network cooperation within the network of pioneerss be further strengthened?

4. Look at the overview below and indicate which five success factors you think are most important. Try to come up with a top five.

Success factor	**Indicator success factor**
Network genesis	According to members, the network started bottom-up.

Objectives consensus	There is agreement among members in the network on objectives.
Autonomy versus direction	There is balance in members' opinions and direction from members in the network.
Clarity about direction	There is clarity on network outcomes and who is directing.
Clarity about own role	There is clarity about one's own role and relationship with other members of the network.
Room for development	The network member is given space from their own organisation and room for new developments within the network.
Access to resources (money/capacity)	Network resources (money/capacity) are contributed by the entire network
Presence of relational factors	There is mutual trust, respect, honesty/reliability in the network. Thereby, everyone is up to cooperation.
Insight into interdependence	Network members are aware that they depend on each other to achieve success on the network objectives.
Mutual language and culture	Network members are aware of the organisational culture, methods, they brings with them and understands those of the other members.
Mutual power relations	Network members have their own influence on decisions taken.
Previous history of the network	Network members have previous positive experiences with network collaborations.
Assurance of participants	From the members, there is long-term commitment to participation from the network.
Appropriate political/policy context	The goals of networking are in line with current politically relevant issues.
Preventing partnership fatigue	Network members feel that there is progress in the network and are not affiliated to many networks themselves.

End of interview

This is the end of the interview. Do you have any suggestions or otherwise comments regarding this topic that we did not discuss in the interview, but that you would like to share?

APPENDIX IV Interview protocol RBPO stakeholder

First of all, thank you for participating in this research. This research provides more insight into how, based on success factors of, network cooperation can be professionalised. For this purpose, the success factors, known from the literature, are placed on a network collaboration.

You are being interviewed because you represent your organisation in the RBPO. The focus of this interview is on your perspective on the network cooperation taking place at the RBPO Working Group Cybersecurity. You will also be given the space to add your own knowledge on what you think are important success factors of network cooperation. This will help expand the knowledge on success factors.

Important!
- In principle, all input is processed anonymously in a final report. This is also described in the consent form. How would you like to be mentioned in the appendix of this study where the list of respondents is; name/function, position or organisation?
- This interview will be worked out verbatim. Would you still like to receive this for verification?
- This survey will be recorded and then edited verbatim. The recording will be deleted immediately afterwards and the anonymous verbatim recording will be kept and can be used to verify the reliability of the research within the university. Do you consent to a recording?
- Get a consent form signed
- Any further questions?

Start interview

1. How long have you been involved with the RBPO?
2. What is your role within the RBPO?

A. Part 1 Network cooperation

A1 How do you rate previous networking in which you have been personally involved?

A2 When do you think a network adds value?

A3 What are the requirements for a good network?

A4 What risks do you see for your organisation in joining/participating in a network? Downside risk?

A5 How have you organised the mandate of employees in networks within your organisation?

A6 How have you organised employee alignment in networks within your organisation?

A9 To what extent is joining networks within your organisation purposefully used to achieve your own organisational goals?

A10 How do you link your organisation results to the results retrieved from a network. As an organisation, in practice you seem to be judged mainly on results that only suit your organisation, while there are always wicked problems that you cannot solve alone.

B. Part 2: Regional working group Cybersafety

B1 To what extent are you aware of the activities of the RBPO working group cybersecurity?

B2 Do you see the pioneers network as a bottom-up or a top-down initiative? Please explain!

bottom up = employees work collectively to identify problems without being mandated by a leader or policy

top-down = employees are activated/guided by decisions or directions made by leaders at the top of their organisation.

B3 How much space is your employee given to join the network around the cybersecurity working group? Explains

B4 Are there arrangements for the safeguarding of these activities?

B5 To what extent is there feedback from your organisation's representative on progress in the working group?

B6 To what extent do you think it is important that money/time is invested from your organisation in the network around the cybersecurity working group? Please explain!

B7 How do you think money/time should be distributed among members from the organisations joining the RBPO? Think especially about new topics that are not yet in policy/priorities but could have major implications for the organisations.

B8 Do you feel that the network around the cybersecurity working group is producing results that add value? Or on a more abstract level; do you notice that the presence of regional cybersecurity working group makes an impact on the Northern Netherlands? If so, cite examples. How do you think it could be improved?

B9 To what extent do you think tackling online crime is a current politically relevant issue? Explain

---

General questions

1. What do you yourself think is an important factor that determines whether a network collaboration is successful?
2. Look at the overview below and indicate which five success factors you think are most important. Try to come up with a top five.

Success factor	**Indicator success factor**
Network genesis	According to members, the network started bottom-up.
Objectives consensus	There is agreement among members in the network on objectives.
Autonomy versus direction	There is balance in members' opinions and direction from members in the network.
Clarity about direction	There is clarity on network outcomes and who is directing.
Clarity about own role	There is clarity about one's own role and relationship with other members of the network.
Room for development	The network member is given space from their own organisation and room for new developments within the network.
Access to resources (money/capacity)	Network resources (money/capacity) are contributed by the entire network
Presence of relational factors	There is mutual trust, respect, honesty/reliability in the network. Thereby, everyone is up to cooperation.
Insight into interdependence	Network members are aware that they depend on each other to achieve success on the network objectives.
Mutual language and culture	Network members are aware of the organisational culture, methods, they bring with them and understands those of the other members.
Mutual power relations	Network members have their own influence on decisions taken.
Previous history of the network	Network members have previous positive experiences with network collaborations.
Assurance of participants	From the members, there is long-term commitment to participation from the network.
Appropriate political/policy context	The goals of networking are in line with current politically relevant issues.
Preventing partnership fatigue	Network members feel that there is progress in the network and are not affiliated to many networks themselves.

End of interview

This is the end of the interview. Do you have any suggestions or otherwise comments regarding this topic that we did not discuss in the interview, but that you would like to share?

APPENDIX V Informed Consent Form

Thanks for agreeing to be interviewed for the research on network cooperation at the RBPO regional Working group on Cybersecurity Northern Netherlands. Below is a description of how your information will be processed in this research and what data will be kept and deleted. For questions, you can always contact me.

For this research:

- I was informed about the nature, method and purpose of this research in a way that was clear to me;
- I have been given enough time to decide about participation;
- I had the opportunity to ask questions about this study;
- I know that participation is voluntary;
- I know that I can stop participating in the study at any time without giving a reason.
- I consent to the collection, storage and use of my answers to answer the research question in this study;
- I know that the results of this interview may be processed in research
- I know that only to check the scientific integrity of the research can people other than the researchers have access to my collected data;
- I understand that any information I provide in relation to this study will be anonymised, so it will not be directly traceable to me;
- I know that I can have access to how the data will be processed and stored;
- I know that I can access how the data is processed and stored;
- I know that if I withdraw, my data can be used until then, unless I also ask for the data already collected to be deleted;
- I consent to the making of a video/audio recording of this interview. This recording will be securely, automatically converted into a transcript and then deleted.

I agree/disagree with these statements.

Name Position title
…….. ……

The final report will contain a list of all the people interviewed. In what way would you like to be named in it (please circle the appropriate description);

Name and position title only position title anonymously

Space for comments:
…….
:…….
:…….