Collaboration Against Ransomware: Evaluation Melissa

Bibi van den Berg, Daan Weggemans and Manon Nobbenhuis

Universiteit Leiden
Institute of Security and Global Affairs

TABLE OF CONTENTS

1. INTRODUCTION

Ransomware attacks aim to achieve financial gain by extorting individuals or organisations.[1] In a ransomware attack, cybercriminals infiltrate a system and often encrypt critical data; the owner or processor can only regain access to this data after paying a ransom – although payment does not guarantee the decryption of the data.[2] Cybercriminals frequently exfiltrate important documents and/or personal data as part of a ransomware attack to use as leverage in negotiations, for instance, by (threatening to) leak documents or selling or granting access to personal data.[3] While the first ransomware case was reported in 1989, it has proliferated since 2005, initially targeting individuals but later shifting focus to (large) public and private organisations due to the substantially higher potential gains.[4] Since 2015, ransomware attacks have become more complex and professional, the ransom demands have increased exponentially, and the economic and societal impact of this phenomenon has surged.[5, 6]

In 2023, according to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens), 178 organisations in the Netherlands fell victim to ransomware attacks.[7] Two years earlier, in 2021, 107 reports of ransomware attacks were filed.[8] This represents a 66% increase in the number of reported attacks over two years. However, the question remains whether these figures fully capture the scope of the ransomware phenomenon in the Netherlands. According to Blom et al., only 2 to 4% of organisations victimised in 2021 reported the incidents to the police. Their research also highlighted surveys conducted by insurers indicating that 26% of all Dutch companies would have been victimised by ransomware in 2022.[9]

1 The Cybersecurity Dictionary (2021) defines ransomware as malicious software in which «the attackers [hold] data [hostage] from the victim and [use] means of pressure to persuade the victim to pay. That hostage-taking often consists of encrypting the victim's data.» See also: Greenberg, Andy, 2018. «The Untold Story of NotPetya, the Most Devastating Cyberattack in History.» *WIRED*, August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.; Schlette, Daniel, Marco Caselli, and Günther Pernul. «A comparative study on cyber threat intelligence: The security incident response perspective.» *IEEE Communications Surveys & Tutorials* 23, no. 4 (2021): 2525-2556.

2 Opderbeck, David W. "Cybersecurity and Data Breach Harms: Theory and Reality." *Md. L. Rev.* 82 (2022): 1001.

3 There are also examples of attacks where data is no longer encrypted and the criminals are limited to extortion, according to one of the respondents (10) to this study. This too can be included in the scope of Project Melissa to be described in more detail. See also Blom, Tessel. 2023. «Ransomware Attacks on Institutions And Businesses in the Netherlands.» Dialogic. September 12, 2023. https://dialogic.nl/2023/09/12/ransomware-aanvallen-op-instellingen-en-bedrijven-in-nederland/.; Autoriteit Persoonsgegevens (AP), «Rapportage ransomware: Gebrekkige beveiliging maakte twee op de drie getroffen organisaties kwetsbaar», 2024, https://www.autoriteitpersoonsgegevens.nl/system/files?file=2024-10/AP%20rapportage%20ransomware.pdf; Matthijsse, Sifra R., M. Susanne van 't Hoff-de Goede, and E. Rutger Leukfeldt. «Your files have been encrypted: A crime script analysis of ransomware attacks.» *Trends in Organized Crime* (2023): 1-27.

4 Blom, Tessel. 2023. «Ransomware-aanvallen Op Instellingen En Bedrijven in Nederland.» Dialogic. September 12, 2023. https://dialogic.nl/2023/09/12/ransomware-aanvallen-op-instellingen-en-bedrijven-in-nederland/.; Matthijsse, Sifra R., M. Susanne van 't Hoff-de Goede, and E. Rutger Leukfeldt. «Your files have been encrypted: A crime script analysis of ransomware attacks.» *Trends in Organized Crime* (2023): 1-27.

5 Hyslip, Thomas S., and George W. Burruss. "Ransomware." In Handbook on Crime and Technology, pp. 86-104. Edward Elgar Publishing, 2023.; Matthijsse, Sifra R., M. Susanne van 't Hoff-de Goede, and E. Rutger Leukfeldt. "Your files have been encrypted: A crime script analysis of ransomware attacks." *Trends in Organized Crime* (2023): 1-27.

6 Hyslip, Thomas S., and George W. Burruss. "Ransomware." *In Handbook on Crime and Technology*, pp. 86-104. Edward Elgar Publishing, 2023.

7 Autoriteit Persoonsgegevens (AP), 'Rapportage ransomware: Gebrekkige beveiliging maakte twee op de drie getroffen organisaties kwetsbaar', 2024, https://www.autoriteitpersoonsgegevens.nl/system/files?file=2024-10/AP%20rapportage%20ransomware.pdf;

8 Tessel, Blom. 2023. "Ransomware-aanvallen Op Instellingen En Bedrijven in Nederland." Dialogic. September 12, 2023. https://dialogic.nl/2023/09/12/ransomware-aanvallen-op-instellingen-en-bedrijven-in-nederland/.

9 This paragraph shows that there is a great lack of reliable figures on the nature and extent of the ransomware phenomenon in the Netherlands. The variety in figures may indicate that parties use different metrics or calculation models to count or not count an attack. It may also indicate a large "dark number". This means that a phenomenon is not easily quantifiable because, due to inadequate information exchange for example, there is insufficient insight into the totality of that phenomenon. Parties then each perceive only part of the phenomenon. See also: Blom, Tessel, 2023. "Ransomware-aanvallen Op Instellingen En Bedrijven in Nederland." Dialogic. September 12, 2023. https://dialogic.nl/2023/09/12/ransomware-aanvallen-op-instellingen-en-bedrijven-in-nederland/.

Falling victim to ransomware is costly, even if an organisation decides not to pay the ransom. Investigating the cause and nature of the incident, managing the aftermath, and restoring systems and networks requires substantial financial, temporal, and human resources.[10] When cybercriminals target large and/or critical organisations, the effects can extend beyond the organisation itself, impacting larger supply chains and citizens. The *Cybersecurity Beeld Nederland* of 2021 identified ransomware as a potential threat to national security for these reasons.[11]

In light of these developments, representatives from the Police, the Public Prosecution Service (OM), the National Cyber Security Centre (NCSC), Cyberveilig Nederland, and some of its members initiated a new collaboration in 2022 to combat ransomware and related forms of cybercrime. This public-private partnership was named 'Melissa.'[12] Within Melissa, parties aim to systematically exchange knowledge and information and collaborate occasionally on specific investigations to collectively contribute to making Dutch public and private organisations less attractive targets for ransomware attacks. Melissa comprises a core group of eleven representatives from the aforementioned organisations. This 'beating heart' of the collaboration prepares sessions and meetings and decides which (new) participants will be involved in Melissa. Surrounding this core group is a layer of representatives from 3 public and 12 private organisations.

In the autumn of 2023, the Melissa collaboration was formalised in a covenant signed by the aforementioned parties. This covenant established the legal, organisational, and technical agreements for the collaboration. It also stipulated that the collaboration would be evaluated. In the summer of 2024, the collaborating partners in Melissa requested Leiden University to carry out this evaluation. The methodology, findings, and recommendations of the evaluation are documented in this report.

Research Questions

This evaluation study focuses on the following questions:

a. Is the logic behind Melissa coherent, and to what extent are the formulated objectives realised in practice?
b. What activities have taken place under the banner of Melissa in recent years, and what results have these led to?
c. What success and failure factors do participants in Melissa identify when reflecting on the past period, and what does this mean for (the organisation of) the collaboration in the coming years, both within Melissa itself and with other public, private, and academic stakeholders, both within and outside the Netherlands?

Approach

The relatively young field of evaluation research has grown significantly in recent years, with many new methods being developed in a short time.[13] For this study, a so-called realistic approach was chosen, which seeks to go beyond the question of whether Melissa works, and instead aims to understand how and why Melissa works in this context. To achieve this, we focus on both the logic of the underlying mechanisms of the project and their practical functioning (see Chapter 2). To gain these insights, various sources and qualitative research methods were employed.

10 Akyazi, Ugur, M. J. G. van Eeten, and C. Hernandez Ganan. «Measuring cybercrime as a service (caas) offerings in a cybercrime forum.» In *Workshop on the Economics of Information Security*. 2021.

11 Nationaal Cyber Security Centrum and Nationaal Coördinator Terrorismebestrijding en Veiligheid. 2021. "Cybersecuritybeeld Nederland 2021." https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021#:~:text=Het%20Cybersecuritybeeld%20Nederland%202021%20(CSBN,daarbij%20op%20de%20nationale%20veiligheid.

12 The name Melissa has its origins in a meeting in the spring of 2022. Here, an incident response party shared an audio clip of a negotiation with a ransomware group. It turned out that the negotiator, who introduced herself as Melissa, had negotiated with some other attendees at earlier times. What stood out d was that these were all other ransomware groups. Thus, one learned that negotiators apparently can be hired by different groups.

13 As aptly described elsewhere previously: "There can be no doubt about it – evaluation is a vast, lumbering, overgrown adolescent" (Pawson, Ray, and Nick Tilley. "An introduction to scientific realist evaluation." *Evaluation for the 21st century: A handbook* 1997 (1997): 405-18.)

Document analysis

For this study, the available documents from the Melissa project were reviewed. This includes official documents such as the covenant, the project plan, action points from the core group meetings, and presentations and reports from meetings held with all participants. Additionally, several publications from the project (white papers on data exfiltration in cyberattacks and ransomware insights) and media reports were analysed. These documents were studied to gain insight into both the underlying theory and the practice of collaboration and information exchange. A list of the consulted documents can be found in Appendix 2.

Interviews

In total, 13 interviews were conducted with various stakeholders involved in the project. These included discussions with members of the core group regarding, among other things, the assumptions underlying the Melissa project. These conversations were important in developing the theoretical assumptions discussed in the second part of this report. Secondly, interviews were held with professionals working at one of the collaborating parties who had been actively involved in Melissa during this period. For example, they attended the organised (two-day) meetings and various sessions. They also shared online insights with the network on relevant developments and trends. The aim was to gain insights into the main results, experiences, and key lessons within this collaboration.

All interviews were semi-structured in nature. Within this format, specific discussion topics were predetermined, but there was also room to ask follow-up questions or explore additional relevant topics.[14] The interviews were conducted online via MS Teams between June and September 2024 and lasted an average of one hour. A high degree of consistency was observed across the conversations, as respondents independently shared many of the same observations. For the completion of the interview phase—both individually and as a whole—the key criterion was saturation: after a certain point, a (new) conversation yields little new insight. Non-verbatim transcripts were created for all these conversations. The interview guide and a list of the interviewees are included in Appendix 3.

Focus group

At the start of the project, an exploratory focus group was organised with 12 participants. The goal was to identify relevant themes for the interview guide and to gather initial shared insights. The focus group also discussed expectations regarding the evaluation study itself. A report on this session, which lasted about an hour, was compiled by the researchers.

Fieldwork: Attending one of the two-day meetings

At the start of the research, the researchers attended one of the two-day Melissa meetings for a few hours. During this visit, they gained an initial understanding of the nature and scope of the collaboration and information-sharing practices within Melissa. Using participatory observation, the researchers mapped out the types of sessions in which participants shared knowledge, the topics they discussed, and the knowledge-sharing formats they used. The observation also included an analysis of interpersonal and social dynamics.

Scientific literature

Scientific literature and sources were used to assess the data collected from the documents and interviews - placing them within a broader framework. Existing scientific insights were helpful in reflecting on ideas regarding the operation, utility, and necessity of the collaboration.

Peer Review

The full report was reviewed by two colleagues within our field, who acted as critical readers. We are grateful to Dr. Tommy van Steen and Dr. Cristina del Real for providing relevant feedback based on their expertise in cybersecurity and cybercrime.

Reading Guide

This evaluation consists of three parts. The first part discusses the theoretical foundations of the project. We focus on the goals and developed approach (Chapter 2). To what extent are the assumptions about the mechanisms behind Melissa function logically sound and evidence-based? The second part then looks at the practical outcomes (Chapter 3) and the success factors and current risks (Chapter 4). What has been done in practice, and does it align with the set objectives? What has the collaboration ultimately achieved? The third part then looks ahead and explores the key

14 Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage.

opportunities and challenges for this collaboration (Chapter 5). Finally, the main conclusions of this evaluation are discussed (Chapter 6).

2. BACKGROUND AND ASSUMED FUNCTIONING

In the first part of this evaluation, we examine the expectations regarding the Melissa collaboration: what were the goals of this collaboration, and what assumptions underpinned it? We will first explore the broader developments in the field of ransomware and the societal context in which the initiative for Melissa emerged. We will then discuss the general design and structure of Melissa. Following this, we describe the analytical framework that guided the evaluation.

Context and Developments

Ransomware is the most common form of cybercrime worldwide.[15] In a ransomware attack, perpetrators hold data from individuals or organisations hostage, demanding a ransom in exchange for its release. To achieve this, malware is used to encrypt the victim's data or system files; these are only released once the victim pays the ransom.[16] Furthermore, a ransomware attack often involves the exfiltration of (important) data, which the perpetrator can then use as leverage to force payment, for example, by threatening to release personal data to the public or sell it, or by leaking sensitive information to the media.[17] [18] In the literature, this is referred to as "double" or even "triple extortion."[19]

Ransomware attacks can cause serious damage. Organised networks of cybercriminals victimize many targets daily by disrupting business operations and stealing data to demand large sums of money.[20] In a targeted and carefully planned attack, this can amount to millions of euros for the victim.[21] For instance, the WannaCry ransomware in 2017 infected 230,000 devices and caused $4 billion in damages worldwide.[22] It is now estimated that the total cost of ransomware attacks could reach tens[23], if not hundreds of billions of dollars.[24] However, the impact of ransomware attacks goes beyond the financial consequences for victims. As has been stated elsewhere: "Ransomware's effects are not just monetary, as the loss of the files themselves (or the costs of ransom) may be eclipsed by the loss of 'client trust, relationships, and reputation.'"[25] In addition, potentially unsafe situations can arise, such as when hospitals or energy plants fall victim to a ransomware attack, halting

15 O'Kane, Philip, Sakir Sezer and Domhnall Carlin. "Evolution of ransomware". *Iet Networks* 7, no. 5 (2018): 321-327.; Oz, Harun, Ahment Aris, Albert Levi, and A. Selcuk Uluagac. "A survey on ransomware: Evolution, taxonomy, and defense solutions."ACM Computing Surveys (CSUR)54, no. 11s (2022): 1-37.; Brewer, Ross. "Ransomware attacks: detection, prevention and cure." *Network security* 2016, no.9 (2016): 5-9.

16 Nationaal Cyber Security Centrum. 2024. "Ransomware." Wat Kun Je Zelf Doen? | Nationaal Cyber Security Centrum. Juni 14, 2024. https://www.ncsc.nl/wat-kun-je-zelf-doen/dreiging/ransomware.; Richardson, Ronny, and Max M. North. "Ransomware: Evolution, mitigation and prevention." *International Management Review* 13, no. 1 (2017): 10.

17 Hyslip, Thomas S., and George W. Burruss. "Ransomware." In *Handbook on Crime and Technology*, pp. 86-104. Edward Elgar Publishing, 2023.

18 Cyberveilig Nederland. 2023, Whitepaper Ransomware. https://cyberveilignederland.nl/upload/userfiles/files/CVNL_Ransomware_def.pdf.

19 Matthijsse, Sifra R., M. Susanne van 't Hoff-de Goede, and E. Rutger Leukfeldt. "Your files have been encrypted: A crime script analysis of ransomware attacks." *Trends in Organized Crime* (2023): 1-27.

20 Staatscourant 2023, Officiele bekendmakingen 29185. November 1, 2023 https://zoek.officielebekendmakingen.nl/stcrt-2023-29185.html

21 Nationaal Cyber Security Centrum. 2022. "Factsheet Ransomware." Factsheet | Nationaal Cyber Security Centrum. October 28, 2022. https://www.ncsc.nl/wat-kun-je-zelf-doen/documenten/factsheets/2020/juni/30/factsheet-ransomware.

22 Kumar, P. Ravi, and Hj Rudy Erwan Bin Hj Ramlie. 2021. "Anatomy of Ransomware: Attack Stages, Patterns and Handling Techniques." In *Advances in Intelligent Systems and Computing*, 205–14. https://doi.org/10.1007/978-3-030-68133-3_20.

23 Kumar, P. Ravi, and Hj Rudy Erwan Bin Hj Ramlie. 2021. "Anatomy of Ransomware: Attack Stages, Patterns and Handling Techniques." In *Advances in Intelligent Systems and Computing*, 205–14. https://doi.org/10.1007/978-3-030-68133-3_20

24 Freeze, Di. 2023. "Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031." Cybercrime Magazine. July 10, 2023. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

25 Sherer, James, Melinda McLellan, Emily Fedeles, and Nichole Sterling. 2017. "Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web." *Richmond Journal of Law & Technology* 23 (3). https://jolt.richmond.edu/files/2017/05/Sherer-Final-clean-.pdf. (22).

vital societal processes.[26] In such cases, a ransomware attack on an organisation can have a broader impact on society and national security.[27] Cybercriminals typically want the impact of ransomware to be as large as possible and may threaten to permanently delete or publicly release data.[28] For example, this occurred with the KNVB in 2023 when a ransomware group threatened to leak the personal data of trainers and players from the Dutch Football Association.[29]

Ransomware is 'big business', and the threat has grown significantly worldwide in recent years. The number of attacks, average downtime, ransom amounts, and total damage have all increased substantially. It is estimated that it takes between 16 and 23 days on average for organisations to resume their activities after an attack.[30] The majority of registered cyber incidents in the Netherlands are ransomware-related. Some notable ransomware attacks in the Netherlands include those targeting container terminals in the Port of Rotterdam (June 2017), Maastricht University (December 2019), the Municipality of Hof van Twente (December 2020), the Netherlands Organisation for Scientific Research (NWO, February 2021), ROC Mondriaan (August 2021), Mediamarkt (November 2021), ID-Ware (September 2022), and the aforementioned attack on the KNVB (September 2023). Cyberveilig Nederland previously stated that 90% of the incident response capacities within the Dutch information security sector were deployed in 2021 for organisations that were victims of a ransomware attack.[31]

These and other attacks in the past decade demonstrate that ransomware has grown in both scale and complexity. In a joint whitepaper, Cyberveilig Nederland, the Police, and the National Cyber Security Centre (NCSC) referred to 'police ransomware' from 2011.[32] In these attacks, computers were locked, and a police logo appeared on the screen, with a message claiming that child pornography had been found. To regain access, a “fine” had to be paid via anonymous online payment methods. The goal here was also to instil as much fear as possible into the victims so that they would pay. In the early years, ransomware attacks were often opportunistic and simplistic in nature: files were not always actually encrypted, and the computer could often be relatively easily restored.[33] But much has changed since then, and cybercriminals have become highly specialised and professional.[34] For example, much has been published recently about the development of Ransomware-as-a-Service (RaaS), where individuals or groups can purchase various services within a well-organised criminal chain.[35] The NCSC (2020) also wrote about how groups have

26 Sherer, James, Melinda McLellan, Emily Fedeles, and Nichole Sterling. 2017. “Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web.” *Richmond Journal of Law & Technology* 23 (3).

27 Tessel, Blom Wazir Sahebali, Kimberly Deppe, Peter Romijn, Floris Donath, and Reg Brennenraedts. 2023. «Ransomeware-aanvallen op instellingen en bedrijven in Nederland.» 2022.173-2319. Dialogic. https://repository.wodc.nl/bitstream/handle/20.500.12832/3292/3375-ransomware-aanvallen-op-instelllingen-en-bedrijven-volledige-tekst.pdf?sequence=7&isAllowed=y. (21)

28 Nationaal Cyber Security Centrum. 2022. “Factsheet Ransomware.” Factsheet | Nationaal Cyber Security Centrum. October 28, 2022. https://www.ncsc.nl/wat-kun-je-zelf-doen/documenten/factsheets/2020/juni/30/factsheet-ransomware.

29 NOS. 2023. «‘Ransomwaregroep Dreigt KNVB Contracten Van Trainers En Spelers Te Lekken.’» April 17, 2023. https://nos.nl/artikel/2471789-ransomwaregroep-dreigt-knvb-contracten-van-trainers-en-spelers-te-lekken.

30 August, Terrence, Duy Dao, and Marius Florin Niculescu. 2022. “Economics of Ransomware: Risk Interdependence and Large-Scale Attacks.” *Management Science* 68 (12): 8979–9002. https://doi.org/10.1287/mnsc.2022.4300. (p. 8980) ; Cyberveilig Nederland. 2023. “Ransomware.” https://cyberveilignederland.nl/upload/userfiles/files/CVNL_Ransomware_def.pdf.

31 Cyberveilig Nederland. 2023, ibid.

32 Cyberveilig Nederland. 2023, ibid (p.7); Dergelijke politie-ransomware werd in meerdere landen gebruikt. For a brief international review, see: O’Gorman, Gavin, and Geoff McDonald, 2012.. “Ransomware: A Growing Menace.” Symantec.

33 Ibid.

34 O’Kane, Philip, Sakir Sezer, and Domhnall Carlin. 2018. “Evolution of Ransomware.” *IET Networks* 7 (5): 321–27. https://doi.org/10.1049/iet-net.2017.0207.

35 Akyazi, Ugur, M. J. G. van Eeten, and C. Hernandez Ganan. “Measuring cybercrime as a service (caas) offerings in a cybercrime forum.” In *Workshop on the Economics of Information Security*. 2021.; Hyslip, Thomas S., and George W. Burruss.

specialised in gaining access to networks or exploiting this access and selling it to interested parties.[36] This allows criminals with limited programming skills to participate and profit from ransomware.[37]

The complexity of ransomware attacks is expected to continue to grow, and cybercriminals will keep developing new methods to maximise profits and minimise risks.[38] Ransomware, in other words, is a dynamic phenomenon involving numerous targeted and untargeted attacks by a network of various parties.[39] Literature often emphasises that it is difficult for the police and judiciary to obtain a full picture of ransomware operations. Actors are often technically difficult to trace, and there is usually a high degree of anonymity, especially as victims are typically asked to pay the ransom in bitcoins or other cryptocurrencies.

Moreover, issues such as “under-reporting” by victims, reluctance to share information about ransomware, and the capacity of law enforcement and judicial services all contribute to investigations sometimes being delayed.[40] As a result, the quality and volume of information remain limited, making it difficult to develop an appropriate and effective response.[41] The literature also highlights the importance of a broad approach where public and private parties from different backgrounds collaborate to prevent and combat ransomware attacks.[42] It is concluded, for example, that both technical and legal expertise on ransomware need to be brought together for a thorough analysis and appropriate response.[43] However, it is often noted that developing such an approach in practice is not straightforward, due to existing legal barriers or conflicting interests and competition between the involved parties.[44]

Melissa: A public-private partnership against ransomware

The Melissa project is a public-private partnership (PPP), which means it is a collaboration between public and private parties. In such collaborations, there is almost always an agreement between the parties to work towards a common goal, where information sharing

“Ransomware.” In *Handbook on Crime and Technology*, pp. 86-104. Edward Elgar Publishing, 2023.; Blom, Tessa, Wazir Sahebali, Kimberly Deppe, Peter Romijn, Floris Donath, and Reg Brennenraedts. 2023. “Ransomeware-aanvallen op instellingen en bedrijven in Nederland.” 2022.173-2319. Dialogic. https://repository.wodc.nl/bitstream/handle/20.500.12832/3292/3375-ransomware-aanvallen-op-instelllingen-en-bedrijven-volledige-tekst.pdf?sequence=7&isAllowed=y. Meland, Per Håkon, Yara Fareed Fahmy Bayoumy, and Guttorm Sindre. 2020. “The Ransomware-as-a-Service Economy Within the Darknet.” *Computers & Security* 92 (May): 101762. https://doi.org/10.1016/j.cose.2020.101762.

36 Nationaal Cyber Security Centrum. 2022. «Factsheet Ransomware.» Factsheet | Nationaal Cyber Security Centrum. October 28, 2022. https://www.ncsc.nl/wat-kun-je-zelf-doen/documenten/factsheets/2020/juni/30/factsheet-ransomware.

37 Meland, Per Håkon, Yara Fareed Fahmy Bayoumy, and Guttorm Sindre. 2020. “The Ransomware-as-a-Service Economy Within the Darknet.” *Computers & Security* 92 (May): 101762. https://doi.org/10.1016/j.cose.2020.101762.

38 Cyberveilig Nederland. 2023. “Ransomware.” https://cyberveilignederland.nl/upload/userfiles/files/CVNL_Ransomware_def.pdf ; 2018b. “Evolution of Ransomware.” IET Networks 7 (5): 321–27. https://doi.org/10.1049/iet-net.2017.0207.

39 Meland, Per Håkon, Yara Fareed Fahmy Bayoumy, and Guttorm Sindre. 2020. «The Ransomware-as-a-Service Economy Within the Darknet.» *Computers & Security* 92 (May): 101762. https://doi.org/10.1016/j.cose.2020.101762.

40 Ministerie van Justitie en Veiligheid. 2024. “Cyberrechercheurs Voor Één Dag.” Reportage | Opportuun. February 9, 2024. https://magazines.openbaarministerie.nl/opportuun/2024/01/politiehackathon.; Robles-Carrillo, M., and P. García-Teodoro. 2022. “Ransomware: An Interdisciplinary Technical and Legal Approach.” Security and Communication Networks 2022 (August): 1–17. https://doi.org/10.1155/2022/2806605; Institute for Security and Technology, 2021. “Combating Ransomware.” https://www.in.gr/wp-content/uploads/2021/05/RTF.pdf.

41 NCTV, «Nederlandse Cybersecuritystrategie 2022-2028.» Nationaal Coördinator Terrorismebestrijding En Veiligheid. https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028.

42 Robles-Carrillo, M., and P. García-Teodoro. 2022. “Ransomware: An Interdisciplinary Technical and Legal Approach.” Security and Communication Networks 2022 (August): 1–17. https://doi.org/10.1155/2022/2806605.

43 Robles-Carrillo, M., and P. García-Teodoro. 2022. «Ransomware: An Interdisciplinary Technical and Legal Approach.» Security and Communication Networks 2022 (August): 1–17. https://doi.org/10.1155/2022/2806605.

44 Robles-Carrillo, M., and P. García-Teodoro. 2022. «Ransomware: An Interdisciplinary Technical and Legal Approach.» Security and Communication Networks 2022 (August): 1–17. https://doi.org/10.1155/2022/2806605; Benmalek, Mourad. 2024. «Ransomware on Cyber-physical Systems: Taxonomies, Case Studies, Security Gaps, and Open Challenges.» Internet of Things and Cyber-Physical Systems, January. https://doi.org/10.1016/j.iotcps.2023.12.001.

is typically a key component. Due to the complexity and far-reaching consequences of cyberattacks, PPPs are regarded worldwide, both within and outside the academic sphere, as a recommended solution.[45] These collaborations are thought to remedy the fragmentation of information spread across various parties. The Dutch Cybersecurity Strategy 2022-2028 (NLCS) explicitly mentions that information exchange is fragmented, meaning organisations may not receive threat information in time, which could prevent them from taking the necessary actions.[46]

Strengthening the information position of parties involved in combating ransomware was also a key objective for Melissa. As stated in the covenant:

> "Currently, there is insufficient insight into the scale of the ransomware threat and related forms of cybercrime in the Netherlands, due to a lack of information (sharing) between and joint analysis by the parties involved in combating this type of cybercrime. Parties hold 'pieces of the puzzle', but these are not being put together effectively. This hampers effective combatting."[47]

Various scientific studies suggest that there is often a certain tension within PPPs, characterised by organisational boundaries and differing interests and powers on one hand, and a shared sense of urgency on the other.[48] This makes collaboration between public and private parties often complex, costly, and vulnerable. Nevertheless, we are seeing increasing attempts to form such collaborations in various sectors.

A realistic analytical framework

Various assumptions, whether implicit or explicit, underpin the design and functioning of Melissa. The realistic approach describes these assumptions and how a programme or project is based on a particular logic that explains how a certain effort will lead to the desired outcome. This logic takes the form of a series of "if-then" premises put forward by the initiators. Therefore, we first examine the causal mechanisms of Melissa and how the actions undertaken should theoretically contribute to achieving the set goals. These mechanisms form the 'engine' of the project and provide an explanation for a particular outcome or result.

This analysis is primarily based on the formal documents from the project itself, such as the covenant and project plan. In addition, in-depth discussions were held with core group members who were involved in the establishment of the collaboration and continue to play a role in its current implementation. These conversations provided more insight into the development and establishment of Melissa and helped uncover any implicit assumptions. The representation below is thus not based on our own (normative) interpretations, but rather directly from the project sources and the experts involved. Later in this chapter, we further examine the theoretical foundation of these causal mechanisms: to what extent is the project both theoretically- and evidence-based? We assess the theoretical assumptions found by comparing them with (scientific) literature and broader societal insights.

45 Carr, Madeline. "Public–private partnerships in national cyber-security strategies." *International Affairs* 92, no. 1 (2016): 43-62.; Boeke, Sergei. "National cyber crisis management: Different European approaches." *Governance* 31, no. 3 (2018): 449-464.; Weiss, Moritz, and Vytautas Jankauskas. "Securing cyberspace: How states design governance arrangements." *Governance* 32, no. 2 (2019): 259-275.; Luiijf, Eric, Kim Besseling, and Patrick De Graaf. "Nineteen national cyber security strategies." *International Journal of Critical Infrastructures* 6 9, no. 1-2 (2013): 3-31.; Shackelford, Scott J., Anjanette Raymond, Danuvasin Charoen, Rakshana Balakrishnan, Prakhar Dixit, Julianna Gjonaj, and Rachith Kavi. "When toasters attack: A polycentric approach to enhancing the security of things." U. Ill. L. Rev. (2017): 415.; Van den Berg, Bibi, and Sanneke Kuipers. "Vulnerabilities and cyberspace: A new kind of crises." *Oxford Research Encyclopedia of Politics* (2022); Christensen, Kristoffer Kjærgaard, and Karen Lund Petersen. "Public–private partnerships on cyber security: a practice of loyalty." *International Affairs* 93, no. 6 (2017): 1435-1452.

46 NCTV. "Nederlandse Cybersecuritystrategie 2022-2028." Nationaal Coördinator Terrorismebestrijding En Veiligheid. https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028.

47 Convenant Melissa (2022).

48 Christensen, Kristoffer Kjærgaard, and Karen Lund Petersen. «Public–private partnerships on cyber security: a practice of loyalty." *International Affairs* 93, no. 6 (2017): 1435-1452. Carr, Madeline. "Public–private partnerships in national cyber-security strategies." *International Affairs* 92, no. 1 (2016): 43-62. Dunn-Cavelty, Myriam, and Manuel Suter. "Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection." *International Journal of Critical Infrastructure Protection* 2, no. 4 (2009): 179-187.

Description: What is the concept behind Melissa?

The goal of Melissa is to make the Netherlands a less attractive target for ransomware attacks.[49] This overarching goal is consistently mentioned in the reviewed documents as well as in the interviews and focus group. The covenant states that this goal involves improving the efficiency and effectiveness of:

- The likelihood of disrupting criminal activities and increasing the chances of offenders being apprehended;
- Providing actionable perspectives for society;
- Supporting (potential) victims within the ransomware attack chain.

Based on the project plan and additional discussions, the researchers distinguish two dimensions of the main objective:

- Increasing the risks and costs for perpetrators of cyberattacks: improving the likelihood of offenders being caught and criminal activities being disrupted.
- Enhancing the resilience of victims and society: providing actionable perspectives for society and supporting (potential) victims within the ransomware attack chain.[50]

The documents do not suggest a hierarchy between these two dimensions; both are central to the collaboration.

To achieve this objective, two main resources are employed:

- Structured knowledge and information sharing about ransomware threats and incidents.
- Improved collaboration between the government and the cybersecurity industry on this issue.

The assumed operational mechanism is that collaboration in combating ransomware will improve when parties get to know each other better and build trust. To facilitate this, processes and procedures must be developed. In order to collaborate effectively, three tracks have been identified within Melissa:

1. A technical/substantive track, which includes the establishment of a communication channel and a MISP (Malware Information Sharing Platform) environment;
2. A legal track, which involves developing the non-disclosure agreement (NDA) and the collaboration covenant and monitoring legal challenges;
3. A practical/organisational track, which focuses on organising meetings, formalising processes and rules of conduct, and communicating results collectively.

49 Convenant Melissa (2022), p.4

50 Convenant Melissa (2022), p. 6; internal documents.

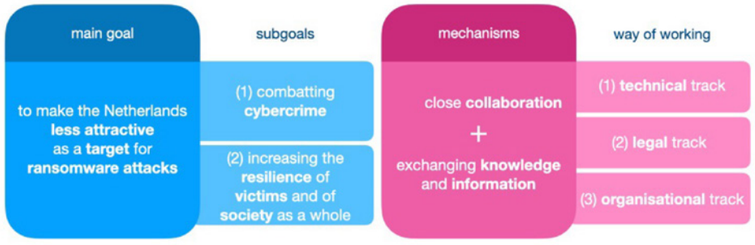

Figure 1: Analytical framework for Melissa

Regarding the exchange of information between the involved parties, the aim is to obtain a more comprehensive view of the attack chain. This can be done through (statistical) research and systematically sharing relevant operational and tactical insights, as well as conducting joint analyses (of phenomena or incidents). The collaboration places great emphasis on trust, confidentiality, legality, and the protection of (sensitive) data. For this reason, various safeguards are in place to ensure "protection of personal data and prevention of improper access."[51]

The goals and assumed mechanisms of Melissa are presented in Figure 1. Throughout this report, we will refer back to this analytical framework when discussing the outcomes, success factors, risks, and future challenges.

Evaluation: Melissa in Theory

The increasing threat of ransomware attacks was the primary impetus for the creation and collaboration within Melissa. This collaboration was intended to improve the shared understanding of the nature and scale of the ransomware threat in the Netherlands.[52] Scientific literature strongly supports the growing complexity of ransomware attacks and the importance of new initiatives in addressing this issue. A key theme within the current state-of-the-art is the intensification of public-private cooperation in this area. Despite many open questions, there is general consensus that collaboration between government bodies (such as the police and the public prosecution service) and private parties is essential for effectively combating ransomware attacks.[53] As the Institute for Security and Technology stated in a recent report: "stopping the flow of ransomware attacks requires a whole-of-society approach. Governments and the private sector alike have highlighted the need to enhance collaboration between government, law enforcement, and the private sector in order to effectively combat ransomware."[54]

However, how such collaborations should be established, the form they should take, and how they can be made sustainable is often underexplored in the literature. It is frequently stated in abstract terms that public-private collaboration can play a vital role in reducing the threat of ransomware, but without further elaboration.[55] Information sharing is often mentioned

51 Convenan Melissa, 2.2

52 Convenant Melissa, p. 2.

53 Laitinen, Marja, and Sarah Armstrong-Smith. "Tackling cybercrime and ransomware head-on: Disrupting criminal networks and protecting organisations." *Cyber Security: A Peer-Reviewed Journal* 5, no. 3 (2022): 190-205; Vish, Elizabeth, and Georgeanela Flores Bustamante. "Public Private Partnerships to Combat Ransomware: An inquiry into three case studies and best practices." https://securityandtechnology.org/virtual-library/reports/public-private-partnerships-to-combat-ransomware/.

54 Vish, Elizabeth, and Georgeanela Flores Bustamante. "Public Private Partnerships to Combat Ransomware: An inquiry into three case studies and best practices." https://securityandtechnology.org/virtual-library/reports/public-private-partnerships-to-combat-ransomware/ p.4.

55 Furthermore, there is additionally a lack of thorough knowledge of, and visibility into, the empirical reality of public-private digital security collaborations, as well as the validation of such collaborations.

as a fundamental pillar of such collaboration.[56] In the Netherlands, the Cyber Security Council (CSR) also argued in 2020 that the cybersecurity landscape is fragmented, and that more cohesion, strength, and speed are needed.[57] Coordinated information exchange is considered essential to strengthen the Netherlands' digital resilience against ransomware and other threats.[58] Scientific publications also recommend that public and private parties enter into agreements to quickly and systematically share information.[59] By structurally sharing insights between public and private organisations, information fragmentation can be avoided, and a clearer threat picture can emerge, leading to more appropriate measures being taken. The existing literature paints a picture of private and public parties studying ransomware attacks in relative isolation, while the importance of collective analysis of the technical, organisational, and practical aspects of ransomware is emphasised to better anticipate new methods and developments.[60]

Thus, the current societal and scientific insights provide a fitting foundation and strong justification for a collaborative initiative like Melissa. The assumption that better collaboration and information sharing between various parties is required to combat ransomware effectively is therefore well-supported by theory.[61]

Furthermore, the assumptions about the functioning of Melissa as an instrument against ransomware are not only theoretically sound but are also, to a certain extent, empirically grounded. As revealed by the documents and interviews, relevant experiences in mutual collaboration were already gained by the involved parties before the establishment of this collaboration. Several interviewees, for example, referred to a meeting in 2021 where representatives from the police, the public prosecution service, the NCSC, Cyberveilig Nederland, and various cybersecurity companies gathered to discuss how they could complement each other in practice. It quickly became apparent that sharing relevant knowledge between professionals yielded valuable insights—not only regarding what is technically possible and legally permissible but also through concrete case studies. For example, information from a private investigator about a server being used by cybercriminals reached the police and prosecution representatives present, and a few days later, the contents of that server became part of the case file. Moreover, exchanges between the various parties led to significant new insights about the organisation of ransomware groups. The covenant, as previously concluded, confirmed and solidified prior experiences and agreements that already seemed to work at an operational level.[62]

56 Christensen, Kristoffer Kjærgaard, and Karen Lund Petersen. «Public–private partnerships on cyber security: a practice of loyalty.» International Affairs 93, no. 6 (2017): 1435-1452; Carr, Madeline. «Public–private partnerships in national cyber-security strategies.» International Affairs 92, no. 1 (2016): 43-62.

57 Cyber Security Raad, 2020. "CSR Jaaroverzicht 2020", p. 17.

58 Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2022. "Nationale Cybersecuritystrategie 2022-2028". 13 -24.

59 Institute for Security and Technology, 2021. "Combating Ransomware." https://www.in.gr/wp-content/uploads/2021/05/RTF.pdf.

60 Benmalek, Mourad. 2024. "Ransomware on Cyber-physical Systems: Taxonomies, Case Studies, Security Gaps, and Open Challenges." *Internet of Things and Cyber-Physical Systems*, January. https://doi.org/10.1016/j.iotcps.2023.12.001: More proactive insights into adversary tactics, techniques and procedures require continued malware reverse engineering and intelligence sharing between public and private organizations. (..) Sectors tend to examine attacks in isolation rather than collectively identifying cross-vertical ransomware innovations. In-depth collaborative analysis of (..) ransomware code evolution, attack infrastructure, adversarial telemetries and victim profiling is essential for anticipating - and getting ahead of - emerging techniques (..).

61 Conversely, Melissa is a relevant and interesting empirical case in a scientific sense because it is an elaboration of what is recommended in the literature in an abstract sense. In doing so, the covenant and the other documents reveal the mechanisms by which the partnership gives substance to information exchange around this framed theme in a concrete sense. For academics, Melissa is an interesting source for studying, for example, success factors for PPPs, but also the meeting in practice of public and private interests, mandates and frameworks.

62 Holterman, Liesbeth, 2024. "Over 'Melissa.'" In *Opportuun*. https://cyberveilignederland.nl/actueel/liesbeth-holterman-in-oppertuun-over-melissa, .

It was only when there was sufficient evidence confirming the value of further collaboration in this context that the decision was made to formalise it. The establishment of this initiative developed collectively and is the result of the active involvement of relevant experts and organisations. Thus, Melissa follows both a theoretical and evidence-based logic.

3. PRACTICE: OUTCOMES

In this part of the evaluation, we focus on practice: what has been done within the project so far, and what have the outcomes and experiences been? First, we explain the activities that have taken place within Melissa, followed by looking at the concrete results achieved (in part) thanks to this collaboration. These will then be summarised in a table, compared with the goals outlined in the covenant, and discussed in more detail.

What has been done in practice?

The central focus within Melissa is information sharing, and structuring and standardising communication and information exchanges. Information sharing takes several forms, each with its own rhythm and dynamics. For instance, participants share statistics and insights during technical sessions. These initially took place monthly and alternated between online and offline formats, but they now occur every six weeks in person, as this was deemed more effective. During these sessions, a TLP-RED round is discussed concerning specific incidents, where tactics, techniques, and procedures (TTPs) are shared and analysed.[63] Additionally, a joint MISP environment has been set up to keep information current.[64] Online communication channels (Signal and Mattermost) have been established for the involved parties, where developments and trends are shared. Knowledge-sharing sessions are regularly organised in various formats, such as technical exchanges, but also two-day events with all involved parties. In the latter type of event, plenary and track sessions alternate, and participants also strengthen their social ties. During these two-day events, there is space for technical, legal, and practical sessions, and ethical and societal dilemmas are also discussed. All these information-sharing activities align with the sub-goal of jointly contributing to the fight against cybercrime.

In addition, several white papers and other knowledge documents have been published within the collaboration. These white papers provide accessible insights and initial action perspectives for organisations regarding ransomware. They contribute to the other sub-goal: increasing resilience against cybercrime.[65]

For the upcoming period, efforts are focused on further developing MISP for information sharing concerning cyber incidents. This task will be transferred from Cyberveilig Nederland to the NCSC. There is also attention on improving the reporting process for victims of ransomware and creating a cyber hotline, where incident response parties can quickly report an incident to the police for more effective action.

Concrete results

The collaboration has led to several noteworthy outcomes. Below is a summary of some publicly shared results that Melissa has contributed to:

- The police successfully acquired more than 150 decryption keys from the ransomware group Deadbolt during a targeted operation, thanks to a tip from the cybersecurity company Responders.NU.[66]
- One of the largest global botnets, Qakbot, was dismantled during a coordinated international operation by law enforcement authorities. Several private participants from Melissa actively contributed behind the scenes. In the Netherlands, the Public Prosecution Service

63 TLP stands for *Traffic Light Protocol* and refers to a method of classifying data or information and guides the information sharing process. The different categories are *Red, Amber, Green* and *White*. With a TLP Red, the receiver(s) may only share the information with the information provider and fellow receivers. In comparison, with a TLP White, there is no restriction on the dissemination of the information and everything may be shared publicly. A full discussion can be found in the Cybersecurity Dictionary (2021),https://cyberveilignederland.nl/woordenboek#:~:text=Met%20het%20woordenboek%20kunnen%20gebruikers,druk%20met%20een%20nieuwe%20look.

64 MISP stands for *Malware Information Sharing Platform* and is used by organizations to share information about cybersecurity threats between parties. Different parties can input/share their information here so that ultimately a better picture of the threat landscape emerges.

65 See for example: Nederland, 2023. “Data-exfiltratie bij een ransomware-aanval.” Online via https://cyberveilignederland.nl/upload/userfiles/files/VCNL_Whitepaper_Exfiltratie_v3_0_Web.pdf.

66 “Nederlandse Gedupeerden Geholpen in Unieke Ransomware-actie.” n.d. Politie.Nl. https://www.politie.nl/nieuws/2022/oktober/14/09-nederlandse-gedupeerde-geholpen-in-unieke-ransomware-actie.html.

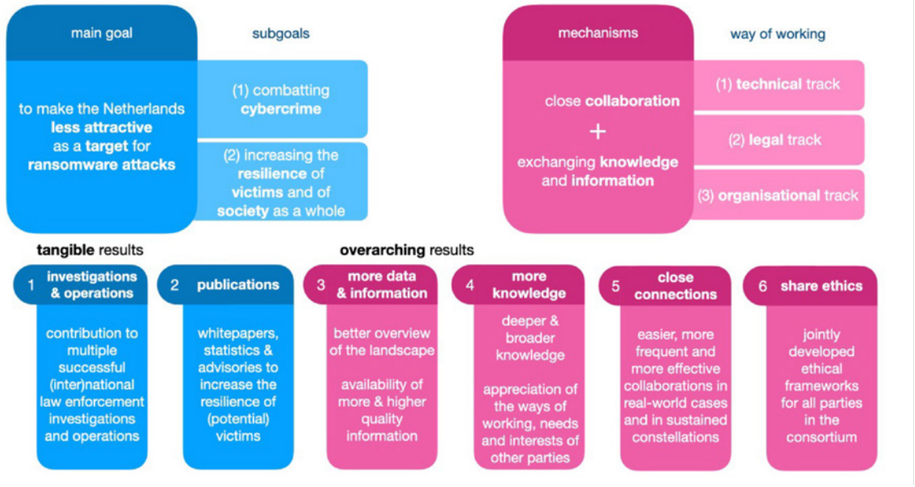

Figure 2: Key outcomes of Melissa

and the police managed to take 22 servers offline.[67]

- The Dutch police contributed to Operation Cookiemonster. This led to the takedown of the criminal trading website Genesis Market by the FBI. The website sold, among other things, social media profiles and bank account information.[68]
- In March 2024, Dutch victims of the ransomware group Cactus were identified. This was made possible by sharing ransomware statistics between parties within Melissa. At least ten Dutch organisations were targeted by Cactus. These organisations were able to take appropriate countermeasures by being informed in time.[69]
- Thanks to a tip from a private party within Melissa, the High Tech Crime team of the Dutch police conducted an investigation into the ransomware group Lockbit. This investigation contributed to an international disruption action.[70]
- The white paper on "Ransomware," published by Cyberveilig Nederland in collaboration with Melissa's partners, provides organisations with insights into ransomware, helping to increase their resilience. [71]
- Additionally, Melissa produced the white paper "Data Exfiltration in a Ransomware Attack." The aim of this document is to provide insight into the exfiltration process used by cybercriminals. With knowledge of this process, organisations can better defend themselves against this phenomenon.

67 Ministerie van Justitie en Veiligheid. 2023. "Grootste Wereldwijde Botnet Qakbot Onschadelijk Gemaakt." Nieuwsbericht | Openbaar Ministerie. September 4, 2023. https://www.om.nl/actueel/nieuws/2023/08/29/grootste-wereldwijde-botnet-qakbot-onschadelijk-gemaakt

68 «Wereldwijd Aanhoudingen Voor Online Identiteitsdiefstal Miljoenen Mensen.» 2023. Politie.Nl. April 5, 2023. https://www.politie.nl/nieuws/2023/april/5/operation-cookiemonster-nl.html.

69 "Samenwerkingsverband Melissa Vindt Diverse Nederlandse Slachtoffers Van Ransomwaregroepering Cactus." n.d. Digital Trust Center (Min. Van EZ). https://www.digitaltrustcenter.nl/nieuws/samenwerkingsverband-melissa-vindt-diverse-nederlandse-slachtoffers-van-ransomwaregroepering.

70 «Servers Neergehaald Van 'S Werelds Grootste Ransomware Groepering.» 2024. Politie.Nl. February 20, 2024. https://www.politie.nl/nieuws/2024/februari/20/09-servers-neergehaald-van-s-werelds-grootste-ransomware-groepering.html.

71 Cyberveilig Nederland, 2023. Whitepaper Ransomware. https://cyberveilignederland.nl/upload/userfiles/files/CVNL_Ransomware_def.pdf.

Overarching Outcomes

In addition to the concrete results mentioned above, several general or overarching outcomes were identified in the interviews. These outcomes of Melissa are schematically presented in Figure 2 above.

Ethical capacity

The collaboration within Melissa has made the ethical boundaries in combating ransomware more visible. Several respondents indicated that through intensive discussions, including those held during knowledge sessions and two-day events, it has become clearer within the consortium which ethical frameworks public and private parties wish to follow in their drive to combat ransomware attacks. The exchanges within Melissa show that safeguarding a shared moral compass is crucial, not only for the collaboration itself but also for the society that benefits from this collaboration. During the discussions, the negative consequences of possible violations by the involved parties were also mentioned. The legal and ethical frameworks have thus been more clearly articulated for all participants in the consortium. A complaints procedure for participants is also being developed.

Finding each other

In addition to the standardised moments when the parties within Melissa have contact with each other, they also regularly speak to each other outside of these moments, for example at a conference or during their daily work. Respondents stated that the lines of communication between the involved public and private parties have become much shorter. Both in formal and informal settings, they now know how to find each other more easily. These shorter lines contribute to a more resilient ecosystem, as current relevant information is quickly and effectively shared between the parties involved. The concrete successes mentioned above are a direct result of the fact that the parties now know how to find each other better and more easily.

Understanding each other's working methods

Because the parties within Melissa are in closer contact with each other, awareness of the different positions, the sometimes conflicting interests, and the varying working methods has grown. Participants stated that they now better know how to approach each other and which information may be relevant to the other. They have also become more familiar with the potential problems that parties face by discussing these together. Through a deeper understanding of each other's interests and working methods, it is possible to better anticipate potential obstacles and parties are better able to work around them.[72]

Improved communication

Through the formalisation of Melissa and the agreements made within this collaboration, a certain maturity has emerged in the collaboration. As a result, internal communication has greatly improved and, according to respondents, a new kind of open conversations has also emerged. Because the same group of people regularly meet, trust within the group has grown, making it "easier to talk to each other and share information," as one participant stated.[73]

72 Respondent 2, Interview

73 Respondent 3, Interview

4. EXPERIENCED SUCCESS AND RISK FACTORS

The results of the collaboration, as discussed in the previous chapter, as well as the collaboration itself, can be explained by a combination of factors that contributed to the positive results achieved. This chapter further explores the explanations for success, as well as the perceived risks for Melissa. What success factors and risks can be identified for Melissa? These success factors, risks, and barriers were shared by respondents during the interviews and the focus group session. In addition, we observed them during the participatory observation at the two-day meeting.

Success factors

We will first focus on the various success factors that emerge from the source material. These relate to a wide range of themes summarised in Figure 3.

Expertise and reciprocity

The expertise and position of the stakeholders involved form an important success factor. According to the respondents, the right number of parties are involved (not too many, not too few), which facilitates quick and easy information exchange. Moreover, the professionals involved have the right knowledge and skills to make a valuable contribution to the project. All involved are expected to share relevant insights, not merely to gather information. The exchange within Melissa is organised on a quid pro quo basis. Of course, it may occur that a stakeholder is unable to contribute during one or a few meetings. However, all respondents agree that if this becomes a recurring issue, involvement within Melissa should be reconsidered. According to the respondents, this principle of reciprocity is one of the conditions for effective collaboration.

Intrinsic motivation and goals

Additionally, it was repeatedly mentioned in the interviews that there is a strong intrinsic motivation among the participants. Most share an almost idealistic view of combating ransomware. For them, making the Netherlands safer and protecting (potential) victims is a priority. Furthermore, individual involvement is generally driven by a strong substantive motivation. Melissa offers an interesting environment where one can learn about all aspects of ransomware and its manifestations. In several interviews, the professionals involved in Melissa were described as "enthusiasts" deeply engaged with the subject matter.[74] This is important because involvement in this collaboration is often voluntary. In other words, there is typically

74 Respondent 5, interview

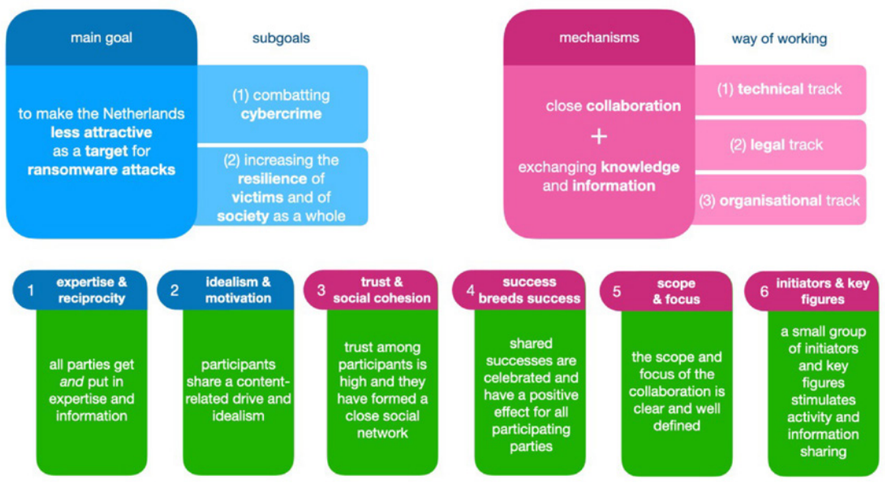

Figure 3: Success factors of Melissa

no budget or hours allocated to the efforts that stakeholders contribute to within Melissa.

Trust and social climate

The positive social climate within Melissa also came up in many interviews. One respondent even referred to it as a "institutionalised Friday afternoon drink."[75] The shared motivation and the fact that there is collaboration within a fixed group contribute to a positive atmosphere within the project. The professionals indicate that they are happy to attend the organised sessions, where there is also ample space for informal conversations. These informal interactions are considered highly important. This also translates into moments outside of Melissa, where the involved professionals frequently encounter each other; the Dutch cybersecurity landscape is, after all, not that large.[76] The ability to collaborate both formally and informally with a relatively stable group fosters trust among the participants.

Success leads to success

Achieving concrete results, such as taking down Genesis Market, also creates a sustained positive atmosphere and high motivation within the group. Respondents also referred to this as a "want-to-be-part-of-this" feeling.[77] Results are seen and celebrated as a collective success, but participants also note that they receive individual recognition for their contributions. This is beneficial for the trust of these organisations, from the perspective of their clients. By communicating the successes of Melissa to clients, trust in the services provided by the organisations grows.

Scope and focus

The Melissa collaboration has a clear boundary, ensuring that the focus remains optimal. This boundary is, on the one hand, content-related: the collaboration focuses on a specific issue, namely ransomware. While ransomware has evolved over time in terms of techniques used, the professionalism of perpetrators, the chosen victims, its scale, and impact, the core of the phenomenon and the goal behind it remain consistent. This provides a stable focus and a clear scope. At the same time, due to the developments surrounding ransomware, there is enough dynamism for the consortium to continue sharing the latest insights and to jointly respond to these developments.

The recognition and handling of ethical and legal frameworks also ensures focus and has a positive effect on the scope of the collaboration. These frameworks provide guidance, helping the consortium remain steadfast in relation to the shared objectives.

Leaders and key figures

Finally, the parties also recognise the role of the leaders of the collaboration. They organise meetings and encourage the parties to actively share information with one another. They also ensure that expectations remain clear. According to the respondents, the success of a PPP should not depend on individuals, but as one respondent pointed out: "Every project has leaders, and you will always need them. This is no different in other sectors."[78]

Existing risks and barriers

Despite good cooperation and the significant successes already achieved with Melissa, the evaluation also provided insight into several risks and barriers that the parties have encountered to date. Figure 4 summarises these risks. Notably, these risks and barriers are closely linked to the success factors.

Investments

Parties involved in the Melissa collaboration participate on a voluntary basis. This means that no hours or financial resources are allocated to the investments and contributions made by the parties. On the one hand, the parties point out that this is an advantage – participation remains accessible, and the collaboration maintains an informal character. On the other hand, it is also seen as a barrier. For example, it is not always possible for the parties to provide information in a timely manner, due to busy periods within their own organisation.

75 Respondent 4, interview

76 Respondent 3, interview

77 Respondent 1, interview

78 Respondent 2, interview

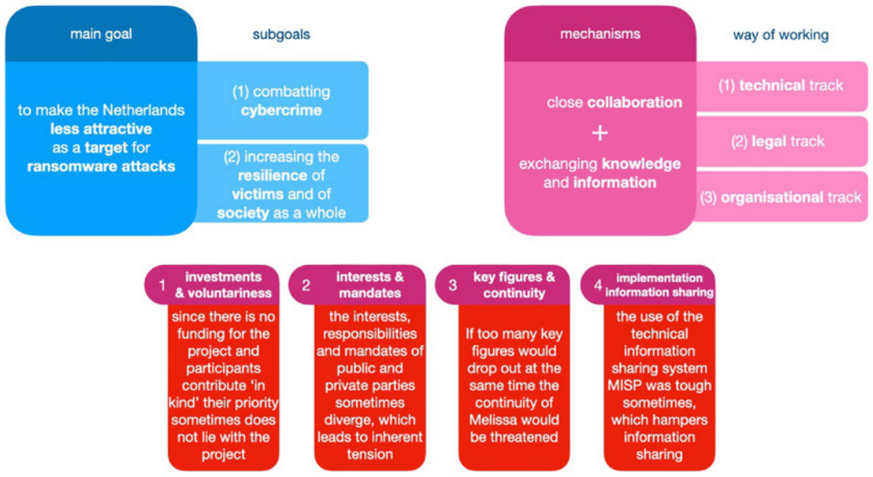

Figure 4: Risks for Melissa

Tension with safeguards and boundaries

In connection with the discussion on ethics, respondents indicated that sharing (sensitive) information sometimes remains complicated. A risk is that certain information cannot or should not be shared with parties, meaning there are limitations on information exchange. This can be a barrier to maximising the collaboration and, more importantly, to effectively combating ransomware attacks. One respondent pointed out that there is a need for legal frameworks that would offer more room for action.[79] However, expanding legal frameworks is easier said than done, and such an expansion must always be weighed against potential risks on one hand and the freedoms and interests of individuals and groups on the other. Moreover, it is uncertain whether expanding legal frameworks is the only solution or whether a reinterpretation of existing legislation or additional agreements between the police, judiciary, and cybersecurity companies could provide sufficient space for more effective ransomware combat.[80] Currently, an exploration of this latter option is underway.

Additionally, it became clear within Melissa that collaboration sometimes also brings ethical dilemmas. Specifically, for the police and judiciary, it can be complicated when information is shared that they cannot use in their line of duty or that may even conflict with their role.[81] Such latent tension may be inherent in the collaboration between public and private parties with differing value structures and sometimes conflicting interests. At the same time, the parties help each other stay sharp by openly discussing this tension, encouraging each other to think about shifting existing boundaries and jointly seeking the maximum leeway that aligns with the moral compass and facilitates motivated action.

Loss of key figures

As mentioned in the section on the outcomes of Melissa, one of the success factors of this PPP is that a small group of key figures play a leading role within Melissa, driving the collaboration and inspiring others. During the interviews, the focus group, and the participatory observation at the two-day meeting, the importance of these key figures was confirmed.

79 Respondent 6, interview

80 Respondent 2, interview

81 Respondent 1, Interview

A risk is that these key figures are difficult to replace when they leave, especially if multiple people leave at the same time. In such a case, there is a chance that the results of the collaboration will be negatively affected, and even the continuity of Melissa may be at risk.[82]

Implementation of the information sharing system

The use of the system for exchanging technical information, MISP, was sometimes problematic. This caused frustration among several parties, as it was not always feasible for them to update the data in the system due to other obligations. As a result, the information-sharing process was delayed, as this data needs to be shared and enriched during the technical sessions. Without this information, the enrichment cannot take place as intended.

82 Respondent 5, interview

5. FUTURE: OPPORTUNITIES AND CHALLENGES

In recent years, notable successes in combating ransomware in the Netherlands have been achieved, partly thanks to the collaboration within Melissa. The previous chapter highlighted potential success factors and risks. The following paragraphs focus on the future of Project Melissa. What opportunities and development questions are emerging? And what (potential) challenges does the collaboration face? Figure 5 schematically outlines the key questions.

From start-up to scale-up?

The period from the inception of informal collaboration, through its consolidation in the signed covenant, to this evaluation moment, marks the first phase of Melissa. During this period, attention was given to setting up the tracks and organisational aspects to promote collaboration. This provided various stakeholders with greater insight into each other's information positions and activities. It facilitated mutual learning among professionals and strengthened networks between the parties.

The coming period will focus more on the development from start-up to scale-up. For instance, will there be an aim for a sustainable embedding of Melissa in the broader Dutch cybersecurity landscape? And if so, how should this be organised? In particular, the future relationship with other public-private collaboration initiatives—such as the Dutch government's Cyclotron programme—was frequently mentioned during the interviews. Ultimately, it seems crucial for structural success that the energy, impact, and perceived autonomy within Melissa are preserved in this growth process. The trust and shared idealism experienced by members are also essential preconditions for a successful future. While integration into a nationwide programme does not appear to be a sensible direction, Melissa can certainly offer valuable lessons for Cyclotron and other PPPs.

In making any decisions about Melissa's future, careful consideration must be given to the impact on the five factors mentioned (energy, impact, autonomy, trust, and shared idealism) and how these can be safeguarded. The further development of Melissa touches on several issues, which we will discuss further below.

Broadening the scope?

The clear scope and focus of Project Melissa have been identified, as mentioned earlier, as one of its success factors. Some consortium members question whether it would be valuable to broaden the project's scope to also share information about other, adjacent cybersecurity themes. The reasoning behind this potential broadening is that various organisations observe other developments that are likely relevant to the parties active within Melissa. While they are eager to share these insights, they feel that the current framework does not always allow for this. The clear delineation as it stands ensures quality, structure, guidance, and normative and legal frameworks; any broadening could put these aspects under pressure.

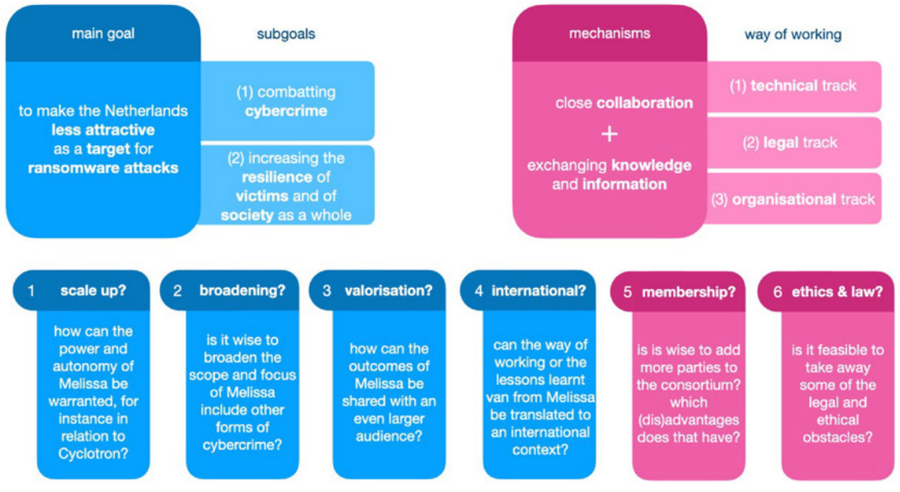

Figure 5: Key questions for (the future of) Melissa

New and existing members?

Melissa has built a strong reputation. Despite the substantial investment required to participate, organisations and professionals express enthusiasm about contributing to the project. Not only do they report gaining valuable insights and forming (or further strengthening) relevant networks, but involvement also seems to offer a certain degree of professional legitimacy. Discussions revealed that organisations enjoy being associated with Melissa, its successes, and its other partners. This is partly the result of consistent, broad recognition of partners' efforts in achieving results. Such positive outcomes generate interest among new potential participants, indicating that the collaboration could grow further in the future.

However, changes in the number of stakeholders involved in Melissa bring both opportunities and challenges. Firstly, it remains important to monitor the contributions of both existing and new members. Are all parties able to consistently share relevant knowledge and information, thereby contributing to effective collaboration? Secondly, excessive changes in membership—through new entries or departures—can impact social cohesion and trust. At the same time, several respondents indicate that there is always room for new participants within Melissa who can make a significant contribution. Recommendations regarding membership, participation, and stakeholder engagement are included in the next chapter.

Crossing borders?

This evaluation has reiterated that ransomware criminals do not adhere to national borders and that they work together in organised international networks. Several stakeholders mentioned during the interviews that maintaining good contact with organisations in other countries is valuable for combating ransomware. Respondents from private entities with international offices, for instance, reported that they regularly gain new knowledge and insights from their foreign partners.

Moreover, during the interviews and focus group discussions, a sense of pride and ownership over Melissa's successes was expressed. This raised the question of whether, and to what extent, a collaboration like Melissa could also be established within and between European countries. In short: could Melissa become an export product? One respondent noted that, while this sounds promising in theory, there are significant "hurdles to overcome."[83] Major legal and administrative differences between countries pose a fundamental barrier to the straightforward establishment of an international equivalent of Melissa that focuses on sharing information among relevant parties. Additionally, cultural differences may hinder the creation of a partnership like the one between public and private stakeholders in the Netherlands. Nevertheless, it remains worthwhile to pursue connections with international partners and to explore how such collaboration could best be structured, with which countries, and involving which international stakeholders.

Ethical dilemmas

As discussed in the previous chapter, Melissa has also brought to light the ethical boundaries and dilemmas in combating ransomware. However, this discussion is far from closed, and it remains essential to jointly seek ethical methods for effective collaboration. For example, it can sometimes be challenging for the police to share certain details, even though some believe this could be beneficial. For commercial parties, sharing information can sometimes be difficult due to the need to protect their business interests. A shared concern is the risk that sensitive information might, in some way, be exposed. Some respondents expressed a desire to do more against ransomware crime than the current frameworks allow. Evaluating the existing frameworks together and informing policymakers and the public about ongoing ethical dilemmas will remain important in the future.

83 Respondent 3, interview

Valorisation and public education

How can the experiences and knowledge gained within Melissa be further disseminated? In the previous period, whitepapers, interviews, and press releases about successful operations have made the ransomware threat more tangible for a broader audience. Such initiatives contribute to achieving the overarching goal of increasing societal and victim resilience. In the future, it will remain essential to make the insights jointly acquired within Melissa accessible to Dutch society. The main challenge lies in ensuring diversity in public outputs and finding a balance with all the other activities within the project.

6. CONCLUSIONS AND RECOMMENDATIONS

Ransomware poses a serious threat to the Dutch government and businesses. The need for effective collaboration is now widely acknowledged and was the catalyst for the creation of the unique Melissa partnership. This chapter reflects on the findings of this evaluation study. We begin by discussing the key conclusions and presenting several recommendations. Finally, we address some general lessons from this project that may be valuable for other (existing or future) collaborations.

Conclusions

The collaboration between public and private parties within Melissa has proven to be highly valuable in combating ransomware. The initiative responded to a landscape characterised by fragmented information and knowledge, which hindered the effective identification and tackling of ransomware threats. Chapter 2 highlighted the theoretical and empirical foundations of Melissa. Both scientific insights and practical developments in the field of ransomware underscore the importance of intensive collaboration between the government and the cybersecurity sector. By prioritising information sharing, knowledge development, and the alignment of workflows and processes, Melissa has successfully translated the recognised necessity for greater collaboration into concrete actions. This has been an incremental process, building on past experiences that laid a solid foundation for the cooperation agreement signed in 2023.

The collaboration within Melissa has manifested in various ways. The most notable are, of course, the successful actions against criminal ransomware groups that received (inter)national media coverage. Additionally, interviews and white papers have been published, contributing to combating cybercrime and enhancing victim resilience. Less visible but crucial to the collaboration are the organised meetings, work sessions, and online exchanges. These activities provided a critical basis for the aforementioned successes and served as a stimulus for professional development and network building. Professionals with varying levels of experience gained new knowledge and insights, enhancing their ability to connect with one another. Moreover, these meetings clarified the ethical frameworks for investigating and combating ransomware throughout the chain, raising awareness of legal boundaries and opportunities.

This evaluation demonstrates that Melissa's broad achievements sometimes exceeded the initially formulated expectations of promoting information sharing and collaboration. The shared belief is that Melissa, regardless of its future course, has had a lasting impact on the cybersecurity sector in the Netherlands.

Finally, the last chapter discussed key success factors and future challenges. Social relationships, trust, clear norms, and a strong sense of shared purpose were identified as the driving forces behind Melissa's successes. Certain members played an indispensable role by driving organisation and setting (and maintaining) norms. Additionally, the successes and shared recognition of everyone's role created momentum and energy within the project.

Partnerships between public and private parties do not arise spontaneously and are no easy feat. This is also true for Melissa. It is an intensive project requiring the structural efforts of the involved stakeholders. This intensity also presents a certain vulnerability. In the coming period, the focus will be on the further development of Melissa, building on the strong foundation now in place.

Recommendations

Based on this evaluation, several recommendations for Melissa's future trajectory can be considered:

Define the project's boundaries and maintain focus

It is tempting to broaden Melissa's scope. Numerous pressing cybersecurity challenges require increased and improved collaboration between organisations. Expanding Melissa's thematic focus could, in theory, allow for the exchange of knowledge and information on other threats. In practice, however, this might dilute attention, jeopardising targeted engagement. A broader collaboration would demand greater resources and involve more parties with diverse expertise, likely increasing the project's complexity and challenges.

Preserve autonomy

One key question concerns Melissa's future relationship with other public-private partnerships (PPPs) in the cybersecurity domain or the national collaborative programme, Cyclotron. From Cyclotron and other bodies, pressure is occasionally exerted to integrate Melissa, generate lessons learned,

or act in an advisory capacity for Cyclotron or other PPPs. Based on Melissa's success factors, it is recommended to carefully safeguard its autonomy. The shared ideology, direct communication, subject-matter expertise, and strong trust base underpin this partnership's success. These factors could be compromised by integration with other initiatives. Sharing lessons learned is undoubtedly valuable, and an advisory role might be interesting, particularly for fostering reciprocity with other PPPs. However, given the limited resources, the scope for such activities must be carefully weighed.

Evaluate membership and admission

For the partnership itself, it is essential to continuously review the structure of membership and admission processes. The ransomware and cybersecurity landscape is dynamic, which may create a need for new expertise and members or cause current members to play a less central role over time. Continuity of individual involvement is considered critical for ensuring trust and recognisability within the partnership. This underscores the importance of evaluating admission and sustainable membership. Ensure that appropriate (vetting) procedures remain in place to facilitate this.

Explore broader involvement

The collaboration within Melissa has led to a solid network of organisations involved in investigating and combating ransomware. While the focus and scale of Melissa should remain limited, it is worthwhile to explore whether other specialised cybersecurity actors could play a peripheral role in the project. This might include professionals who do not meet all membership requirements—such as those lacking relevant information to share—but who possess valuable skills and knowledge. They could form a supportive layer around the project, contributing to knowledge product development, such as white papers, and strengthening relationships within the Dutch cybersecurity domain.

Continue addressing and investigating ethical dilemmas

Melissa has led to several successful joint operations and shared reflections on a moral compass for tackling ransomware. By exchanging information and experiences regarding the legal frameworks in which different parties operate, participants' operational perspectives can become more concrete and refined. Additionally, ethical discussions can highlight instances where practice and the law may conflict. These discussions could serve as a starting point for exploring new approaches or developing policy frameworks. Legal frameworks evolve over time, as do the nature, scale, and impact of ransomware attacks. For this reason, it is crucial to devote structural attention within Melissa to discussing legal and ethical frameworks, ensuring they remain aligned with contemporary legal standards and practices.

Lessons for other partnerships in the cyber domain

The experiences gained within Melissa reveal several general lessons for effective collaboration in cybersecurity. These lessons concern 1) organisation, 2) execution, and 3) outcomes of collaboration.

Organisation: Who is at the table, and under what conditions?

1. Involve a select group of parties with relevant expertise. Bigger is not always better. Social cohesion and trust, on the other hand, are indispensable. Expertise ensures respect and meaningful knowledge exchange, which are crucial for enthusiasm and long-term support.
2. Ensure diversity among participants. This fosters learning and the exchange of insights.
3. Leadership and structured coordination are necessary for organising effective collaboration.
4. Avoid unnecessary participant turnover, but membership is not sacred. If someone cannot contribute structurally to the objectives, involvement might be better shaped differently.
5. Start with a shared purpose and communicate it clearly.
6. Outline clear expectations of the collaboration and set achievable goals.

Execution: How is collaboration implemented?

7. Encourage active and balanced information and knowledge sharing between parties based on a quid pro quo principle.
8. Organise training and knowledge exchange sessions, requiring good preparation and active participation from attendees.
9. Successful collaboration and networking rely on social relationships and trust. Physical meetings and sufficient social elements within projects are thus vital.
10. Establish basic rules (e.g., confidentiality), make them a regular discussion topic, and monitor their adherence.
11. Set clear working agreements and ensure compliance by all parties.
12. Acknowledge that parties have different backgrounds and resources, meaning their contributions may vary.
13. Recognise that parties have different, sometimes conflicting interests. Highlight the shared interest and discuss its boundaries to clarify how collaboration can proceed.

Results: How to handle output?

14. Ensure outcomes are sufficiently tangible for participants, making their efforts meaningful.
15. Share results with each other and, where possible, the public, generously acknowledging each party's role and contribution.
16. Accept that collaboration with numerous parties often requires significant investments of time, energy, and resources.

Collaboration against Ransomware: Evaluation Melissa

LITERATURE

Akyazi, Ugur, M. J. G. van Eeten, and C. Hernandez Ganan. "Measuring cybercrime as a service (caas) offerings in a cybercrime forum." In *Workshop on the Economics of Information Security*. 2021.

August, Terrence, Duy Dao, and Marius Florin Niculescu. 2022. "Economics of Ransomware: Risk Interdependence and Large-Scale Attacks." *Management Science* 68 (12): 8979–9002. https://doi.org/10.1287/mnsc.2022.4300.

Autoriteit Persoonsgegevens (AP), 'Rapportage ransomware: Gebrekkige beveiliging maakte twee op de drie getroffen organisaties kwetsbaar', 2024, https://www.autoriteitpersoonsgegevens.nl/system/files?file=2024-10/AP%20rapportage%20ransomware.pdf;

Benmalek, Mourad. 2024. "Ransomware on Cyber-physical Systems: Taxonomies, Case Studies, Security Gaps, and Open Challenges." *Internet of Things and Cyber-Physical Systems*, January. https://doi.org/10.1016/j.iotcps.2023.12.001.

Blom, Tessel, Wazir Sahebali, Kimberly Deppe, Peter Romijn, Floris Donath, and Reg Brennenraedts. 2023. "Ransomeware-aanvallen op instellingen en bedrijven in Nederland." 2022.173-2319. Dialogic. https://repository.wodc.nl/bitstream/handle/20.500.12832/3292/3375-ransomware-aanvallen-op-instelllingen-en-bedrijven-volledige-tekst.pdf?sequence=7&isAllowed=y.

Boeke, Sergei. "National cyber crisis management: Different European approaches." *Governance* 31, no. 3 (2018): 449-464.

Brewer, Ross. "Ransomware attacks: detection, prevention and cure." *Network security* 2016, no. 9 (2016): 5-9.

Carr, Madeline. "Public–private partnerships in national cyber-security strategies." *International Affairs* 92, no. 1 (2016): 43-62.

Christensen, Kristoffer Kjærgaard, and Karen Lund Petersen. "Public–private partnerships on cyber security: a practice of loyalty." *International Affairs* 93, no. 6 (2017): 1435-1452.

Convenant Melissa (2023). https://zoek.officielebekendmakingen.nl/stcrt-2023-29185.pdf

Cyber Security Raad, 2020. "CSR Jaaroverzicht 2020".

Cyberveilig Nederland. 2021. "Cybersecurity Handboek 2021". https://cyberveilignederland.nl/woordenboek#:~:text=Van%20cybersecurity%20naar%20Nederlands&text=Het%20woordenboek%20blijft%20in%20ontwikkeling,via%20woordenboek%40cyberveilignederland.nl.

Cyberveilig Nederland. 2023. "Ransomware." https://cyberveilignederland.nl/upload/userfiles/files/CVNL_Ransomware_def.pdf.

Digital Trust Center, "Samenwerkingsverband Melissa Vindt Diverse Nederlandse Slachtoffers Van Ransomwaregroepering Cactus." https://www.digitaltrustcenter.nl/nieuws/samenwerkingsverband-melissa-vindt-diverse-nederlandse-slachtoffers-van-ransomwaregroepering.

Dunn-Cavelty, Myriam, and Manuel Suter. "Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection." *International Journal of Critical Infrastructure Protection* 2, no. 4 (2009): 179-187.

O'Gorman, Gavin, and Geoff McDonald, 2012.. "Ransomware: A Growing Menace." Symantec.

Greenberg, Andy, and Excerpt. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." WIRED, 22 augustus, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Freeze, Di. 2023. "Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031." Cybercrime Magazine. July 10, 2023. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

Holterman, Liesbeth, 2024. "Over 'Melissa.'" In Opportuun. https://cyberveilignederland.nl/actueel/liesbeth-holterman-in-oppertuun-over-melissa, .

Hyslip, Thomas S., and George W. Burruss. "Ransomware." In *Handbook on Crime and Technology*, pp. 86-104. Edward Elgar Publishing, 2023.

Institute for Security and Technology. 2021. "Combating Ransomware." https://www.in.gr/wp-content/uploads/2021/05/RTF.pdf.

Kumar, P. Ravi, and Hj Rudy Erwan Bin Hj Ramlie. 2021. "Anatomy of Ransomware: Attack Stages, Patterns and Handling Techniques." *In Advances in Intelligent Systems and Computing*, 205–14. https://doi.org/10.1007/978-3-030-68133-3_20.

Laitinen, Marja, and Sarah Armstrong-Smith. "Tackling cybercrime and ransomware head-on: Disrupting criminal networks and protecting organisations." *Cyber Security: A Peer-Reviewed Journal* 5, no. 3 (2022): 190-205.

Luiijf, Eric, Kim Besseling, and Patrick De Graaf. "Nineteen national cyber security strategies." *International Journal of Critical Infrastructures* 6 9, no. 1-2 (2013): 3-31.

Matthijsse, Sifra R., M. Susanne van 't Hoff-de Goede, and E. Rutger Leukfeldt. "Your files have been encrypted: A crime script analysis of ransomware attacks." *Trends in Organized Crime* (2023): 1-27.

Meland, Per Håkon, Yara Fareed Fahmy Bayoumy, and Guttorm Sindre. 2020. "The Ransomware-as-a-Service Economy Within the Darknet." *Computers & Security* 92 (May): 101762. https://doi.org/10.1016/j.cose.2020.101762.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage.

Ministerie van Justitie en Veiligheid. 2023. "Grootste Wereldwijde Botnet Qakbot Onschadelijk Gemaakt." Nieuwsbericht | Openbaar Ministerie. September 4, 2023. https://www.om.nl/actueel/nieuws/2023/08/29/grootste-wereldwijde-botnet-qakbot-onschadelijk-gemaakt.

Ministerie van Justitie en Veiligheid. 2024. "CyberrechercheursVoorÉénDag." Reportage|Opportuun. February 9, 2024. https://magazines.openbaarministerie.nl/opportuun/2024/01/politiehackathon.

Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2022. "Nationale Cybersecuritystrategie 2022-2028".

Nationaal Cyber Security Centrum en Nationaal Coördinator Terrorismebestrijding en Veiligheid. 2021. "Cybersecuritybeeld Nederland 2021." https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021#:~:text=Het%20Cybersecuritybeeld%20Nederland%202021%20(CSBN,daarbij%20op%20de%20nationale%20veiligheid.

Nationaal Cyber Security Centrum. 2022. "Factsheet Ransomware." Factsheet | Nationaal Cyber Security Centrum. October 28, 2022. https://www.ncsc.nl/wat-kun-je-zelf-doen/documenten/factsheets/2020/juni/30/factsheet-ransomware.

Nationaal Cyber Security Centrum. 2024. "Ransomware." Wat Kun Je Zelf Doen? | Nationaal Cyber Security Centrum. June 14, 2024. https://www.ncsc.nl/wat-kun-je-zelf-doen/dreiging/ransomware.

"Nederlandse Cybersecuritystrategie 2022-2028." Nationaal Coördinator Terrorismebestrijding En Veiligheid. https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028.

NOS. 2023. "'Ransomwaregroep Dreigt KNVB Contracten Van Trainers En Spelers Te Lekken.'" April 17, 2023. https://nos.nl/artikel/2471789-ransomwaregroep-dreigt-knvb-contracten-van-trainers-en-spelers-te-lekken.

O'Kane, Philip, Sakir Sezer, and Domhnall Carlin. "Evolution of ransomware." *Iet Networks* 7, no. 5 (2018): 321-327.

Opderbeck, David W. "Cybersecurity and Data Breach Harms: Theory and Reality." *Md. L. Rev*. 82 (2022): 1001.

Oz, Harun, Ahmet Aris, Albert Levi, and A. Selcuk Uluagac. "A survey on ransomware: Evolution, taxonomy, and defense solutions." *ACM Computing Surveys (CSUR)* 54, no. 11s (2022): 1-37.

Pawson, Ray, and Nick Tilley. "An introduction to scientific realist evaluation." *Evaluation for the 21st century: A handbook* 1997 (1997): 405-18.

Politie,"Servers Neergehaald Van 'S Werelds Grootste Ransomware Groepering." Politie.Nl. februari 20, 2024. Politie.nl. https://www.politie.nl/nieuws/2024/februari/20/09-servers-neergehaald-van-s-werelds-grootste-ransomware-groepering.html (2024).

Politie, "Nederlandse Gedupeerden geholpen in Unieke Ransomware-actie." Politie.nl. https://www.politie.nl/nieuws/2022/oktober/14/09-nederlandse-gedupeerde-geholpen-in-unieke-ransomware-actie.html (2023).

Richardson, Ronny, and Max M. North. "Ransomware: Evolution, mitigation and prevention." *International Management Review* 13, no. 1 (2017): 10.

Robles-Carrillo, M., and P. García-Teodoro. 2022. "Ransomware: An Interdisciplinary Technical and Legal Approach." *Security and Communication Networks* 2022 (August): 1–17. https://doi.org/10.1155/2022/2806605

Schlette, Daniel, Marco Caselli, and Günther Pernul. "A comparative study on cyber threat intelligence: The security incident response perspective." *IEEE Communications Surveys & Tutorials* 23, no. 4 (2021): 2525-2556.

Shackelford, Scott J., Anjanette Raymond, Danuvasin Charoen, Rakshana Balakrishnan, Prakhar Dixit, Julianna

Staatscourant 2023, Officiele bekendmakingen 29185. November 1, 2023. https://zoek.officielebekendmakingen.nl/stcrt-2023-29185.html.

Gjonaj, and Rachith Kavi. "When toasters attack: A polycentric approach to enhancing the security of things." *U. Ill. L. Rev*. (2017): 415.

Sherer, James, Melinda McLellan, Emily Fedeles, and Nichole Sterling. 2017. "Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web." *Richmond Journal of Law & Technology* 23 (3). https://jolt.richmond.edu/files/2017/05/Sherer-Final-clean-.pdf. (22).

Van den Berg, Bibi, and Sanneke Kuipers. "Vulnerabilities and cyberspace: A new kind of crises." *Oxford Research Encyclopedia of Politics* (2022).

Vish, Elizabeth, and Georgeanela Flores Bustamante. n.d. "Public Private Partnerships to Combat Ransomware: An inquiry into three case studies and best practices." https://securityandtechnology.org/virtual-library/reports/public-private-partnerships-to-combat-ransomware.

Weiss, Moritz, and Vytautas Jankauskas. "Securing cyberspace: How states design governance arrangements." *Governance* 32, no. 2 (2019): 259-275.

APPENDIX

Appendix 1: Respondents and affiliation

Name	Organisation
Baars, Esther	Public Prosecution Service
Blokhuis, Joeri	Responders.Nu
Brand, Rosalie	Kennedy Van der Laan
Brouwer, Rayan	Deloitte
Fennis, Joey	Dataexpert
Hensen, Lodi	Eye Security
Jaspers, Matthijs	Police
Keuper, Daan	Computest
Koopman, Gert	NFIR
Oldengarm, Petra	Cyberveilig Nederland
Takkenberg, Pim	Northwave
Van Amelsfort, Matthijs	Police

Appendix 2: Consulted Documents (Project-Specific)

Convenant Melissa (2023). https://zoek.officielebekendmakingen.nl/stcrt-2023-29185.pdf

Cyberveilig Nederland (2023), *Whitepaper Ransomware*. Available online as of November 13, 2024, at https://cyberveilignederland.nl/upload/userfiles/files/CVNL_Ransomware_def.pdf

Cyberveilig Nederland (2023), "*Data Exfiltration in a Ransomware Attack*." Available online as of November 13, 2024, at https://cyberveilignederland.nl/upload/userfiles/files/VCNL_Whitepaper_Exfiltratie_v3_0_Web.pdf

Melissa (2024), *Presentation: Melissa Two-Day Event* 2024.

Melissa (2023), *Presentation: Ransomware Two-Day Event, Legal/Organizational Program*.

Melissa (2023), *Presentation: Approach to Technical Information Sharing - Melissa*.

Melissa (2022), *Presentation: Results and Next Steps of Project Melissa*.

Melissa (2022), *Presentation: Melissa Meeting November 30*.

Melissa (2022), *Presentation: Melissa Captain's Dinner - Summary and Conclusions*.

Melissa (2022), *Presentation: Melissa Project Plan 2022–2023*.

Melissa (2022), *Status of Action Points Melissa a*.

Melissa (2022), *Status of Action Points Melissa b*.

Appendix 3: Interview Topiclist

Introduction:

How were you involved in the project?

What was your role?

Exploratory Evaluation Topics:

Before (Status Quo, Expectations, and Goals):

What were the relationships like before the project?

Can you describe the landscape/situation surrounding ransomware countermeasures in the Netherlands before Melissa?

What was your primary expectation of Melissa?

What was your goal with this collaboration between private and public parties?

Reflection on the Past Period (Results Achieved, Approach, Experiences, and Obstacles):

How did you try to shape the collaboration? What ideas were behind this?

What do you consider the most important outcomes/ achievements?

In your opinion, were the set goals achieved? (If so, what do you think contributed to this?)

What do you see as the key added value of the collaboration?

Were there also obstacles and challenges?

Future (Additional Needs, Long-Term Ambitions):

What is needed to successfully combat ransomware attacks as a society in the future?

What is your perspective on Melissa in the long term?

Universiteit
Leiden
Institute of Security
and Global Affairs

With us you get to know the world