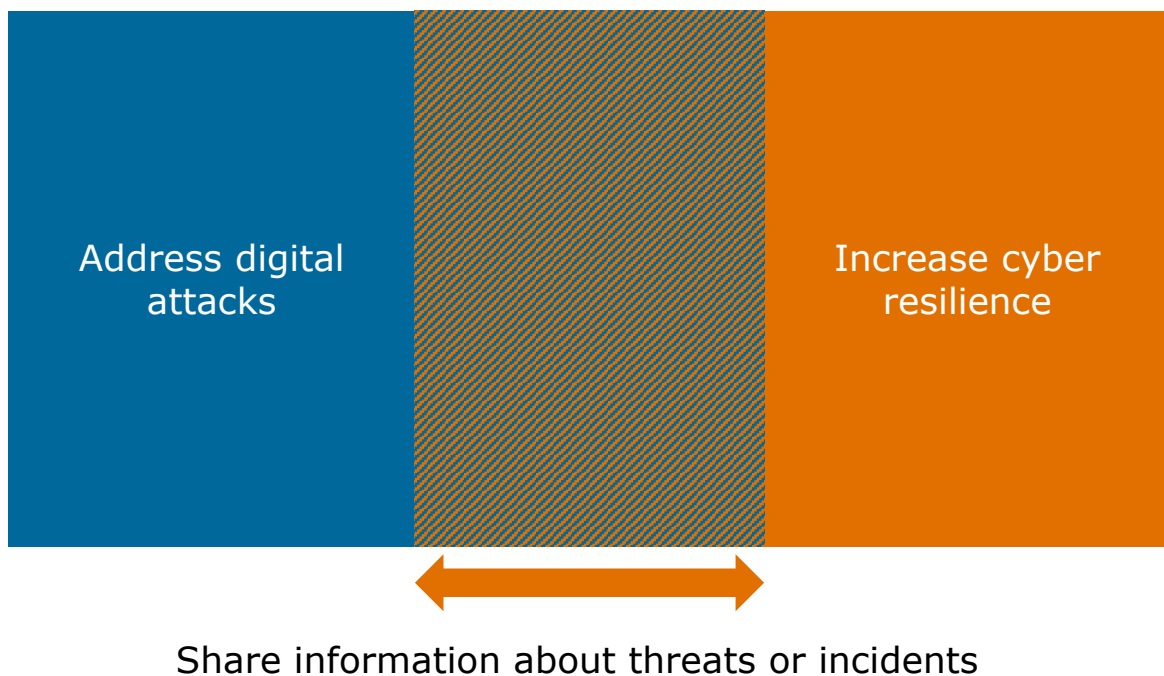


CYCLOTRON

Joining forces in a public-private partnership to achieve faster, more targeted information sharing in relation to cyber incidents



Petra Oldengarm
Lex Mooy
31 May 2022

About the authors

Petra Oldengarm is an independent strategic cybersecurity consultant who advises the government and private organisations on several strategic themes. After graduating from the Groningen University with a degree in Technical Computer Science, she gained experience with various employers in the public and the private sector. Oldengarm has been active in the cybersecurity domain for many years and has worked as an independent consultant since 2018. Besides her consultancy work, Oldengarm is a (part-time) director at Cyberveilig Nederland (the trade association for the Dutch cybersecurity sector) and a guest lecturer at Leiden University. She is also a member of the Supervisory Board of the Dutch Institute for Vulnerability Disclosure (DIVD).

After a stint as a public prosecutor specialising in organised crime and international fraud, Lex Mooy became a judge 18 years ago – based initially at the court of appeal in Den Bosch and now at the court of appeal in Amsterdam. In his present role, Mooy has continued to specialise in organised crime and international fraud. Besides his work as a judge, Mooy has a number of ancillary roles. For example, he chairs several healthcare-related dispute committees, is a legal member of the Central Disciplinary Committee for the Healthcare Sector (*Centraal Tuchtcollege voor de Gezondheidszorg*) and the chair of the Undesirable Conduct Complaints Committee (*Klachtencommissie Ongewenst Gedrag*) of HU University of Applied Sciences Utrecht. He is also a (deputy) justice in the specialist cyber division at the court of appeal in The Hague. For the last four years, Mooy has been a member of the Review Board for the Use of Powers (*Toetsingscommissie Inzet Bevoegdheden*, TIB), which supervises the use of special powers by the General Intelligence and Security Service (*Algemene Inlichtingen- en Veiligheidsdienst*, AIVD) and the Military Intelligence and Security Service (*Militaire Inlichtingen- en Veiligheidsdienst*, MIVD).

TABLE OF CONTENTS

MANAGEMENT SUMMARY	1
INTRODUCTION AND PROBLEM DEFINITION	5
Problem definition	5
RESEARCH QUESTIONS AND READING GUIDE	7
Research questions	7
Reading guide	8
THE CURRENT LANDSCAPE FOR INFORMATION SHARING.....	9
The Dutch landscape for sharing information about cyber incidents.....	9
International initiatives.....	18
National initiatives in other domains.....	20
MORE INTENSIVE INFORMATION SHARING NEEDED.....	21
DESIGN OF THE CYCLOTRON PLATFORM	23
Information needs and objectives	23
Design method	25
Design: information	25
Design: stakeholders.....	28
Design: channels	33
SPECIAL FRAMEWORK CONDITIONS	35

Legal framework.....	35
Organisational structure and Governance	40
Building a trusted community	43

ALIGNMENT WITH THE EXISTING LANDSCAPE 46

Future vision: integration of existing initiatives	46
Relationship with the CIIC.....	47
Relationship with the LDS	48
Relationship with the NDN.....	48
Relationship with SecureNed	49

RECOMMENDATIONS FOR NEXT STEPS..... 51

Use the Cyclotron design as a blueprint	51
EMBED the platform WITHIN the NCSC	51
Start development of the long-term legal framework immediately	52
Establish a governance board and an agenda board.....	52
Make a quick start by linking to SecureNed	52
Design a separate solution for target and victim notification	53

ANNEXES..... 55

Information model	55
Modelling of initiatives in the information sharing landscape	58
Overview of foreign initiatives.....	70
Overview of domestic initiatives in other domains	74
Organisations consulted.....	76
List of abbreviations.....	77

MANAGEMENT SUMMARY

This report presents the results of the exploratory research conducted under the working name 'Cyclotron' between October 2021 and May 2022, and focuses on the following main research question:

What are the possibilities and requirements for strengthening public-private partnerships at an operational and tactical level¹ so that the response to cyber incidents becomes more effective and efficient?

The starting point for the Cyclotron exploratory research project was the observation that **an insufficient amount of information is shared by public and private partners when a cyber incident occurs or is imminent, and that this information is not shared promptly**. This situation must be rectified if **cyber resilience is to be increased** and the **cyber threat reduced**.

The researchers, Petra Oldengarm and Lex Mooy, started by identifying bottlenecks and needs in the current national and international information-sharing landscape. Initiatives in other domains were considered as well. Overall, the researchers concluded that there is an **urgent need for a platform to share information about occurring or imminent cyber incidents more intensively**. When sharing information, a stakeholder network consisting of both public and private parties is important. In the first phase of the exploratory research, the researchers formulated **a large number of needs, challenges and requirements** to be taken into consideration when designing a platform. This functioned as important input for the design the researchers developed in the second phase of their exploratory research.

¹ The remit for the Cyclotron exploratory research project was explicitly limited to cooperation at the operational and tactical level and excluded cooperation at the strategic level.

Information sharing via the Cyclotron platform has the following objective:

To make the Netherlands an unattractive target for digital attacks

The starting point for the design of the Cyclotron platform is the observation that the informational needs that users have are directly proportional to their maturity. The following **two needs** emerged from the analysis of the landscape:

1. **High-maturity organisations** need to **receive unanalysed raw data quickly**.
2. **All organisations** need **analysed information**. The analyses in question could be carried out jointly.

These information needs then translate into three purposes for information sharing: (a) to share raw data quickly – push, (b) to request information – pull, and (c) to analyse information together.

The researchers identified a **broad need to share both operational and tactical information** (see Figure 1). Various requirements were formulated for this information. Although the subject of target and victim notification was placed outside the scope of the Cyclotron platform, the researchers did issue several recommendations in this regard (see *Recommendations for next steps*).

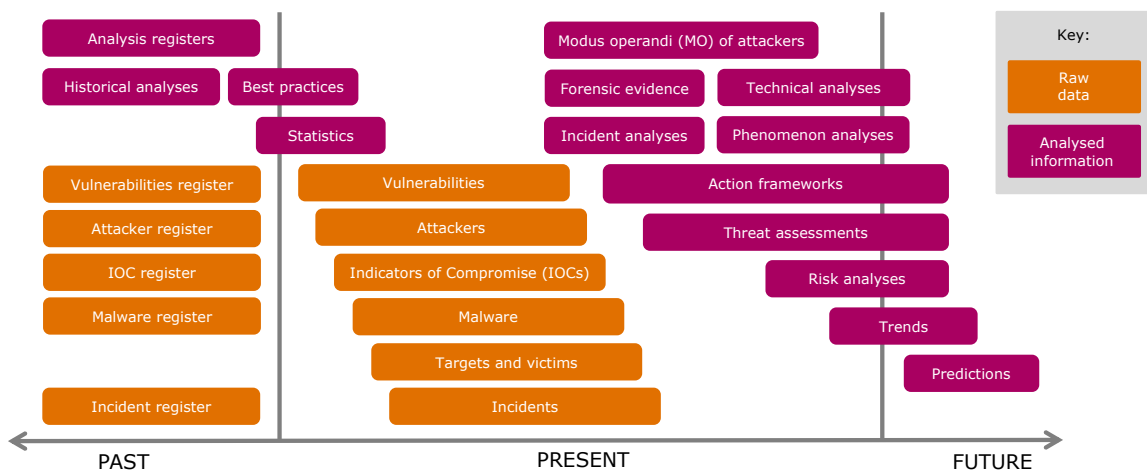


Figure 1 - Selection of the information to be shared

To be able to share information, the following three centres need to be developed (see Figure 2):

1. An **information sharing centre** that will enable high-maturity stakeholders to quickly share raw data with each other.
2. An **analysis and resilience centre** that will focus on conducting joint analyses and providing advice.
3. A **communication and distribution centre** that will focus on aligning communication to users and ensuring that information is distributed.

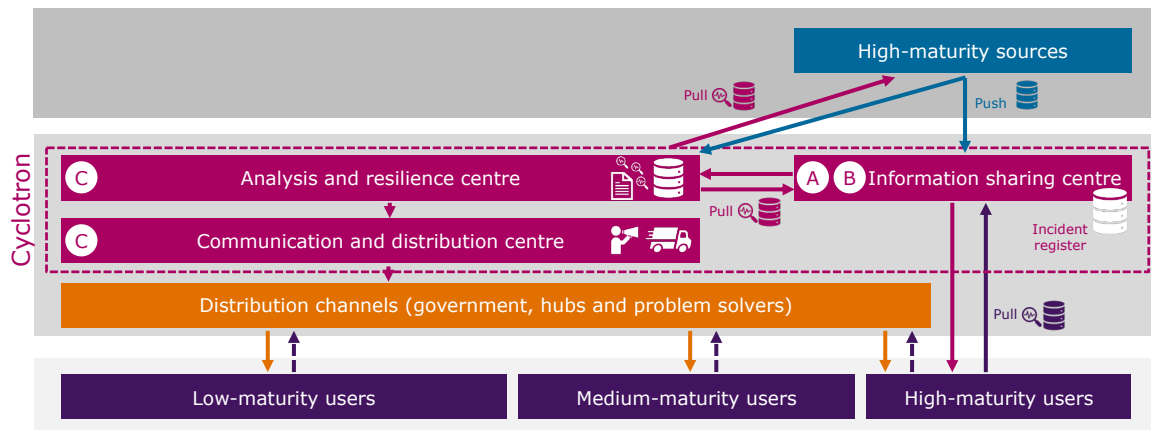


Figure 2 - Stakeholder design for the Cyclotron platform

A number of requirements were defined for the three centres. An important requirement is the ability to share highly confidential information. With this in mind, **the concept of subgroups was developed** in the design, making it possible to **share highly confidential information with a limited circle of users with sufficient safeguards in place.**

Finally, the researchers established the channels necessary to share information and the relevant requirements.

The researchers investigated several of the requirements above in more detail, viz. the legal framework, governance and how to build a trusted community.

The most important conclusion with regard to the legal framework was that it would be **wise to make the Cyclotron platform part of a public organisation. As none of the current legal frameworks can be considered adequate for the activities of the platform, it will also be necessary to develop new legislation.** The researchers recommend that this process start immediately after a positive decision on the development of Cyclotron.

The researchers also recommend that the **Cyclotron platform become part of a lead organisation.** The public organisation most suitable for this purpose is **the national cybersecurity authority**, which is currently being established through the merger of the National Cyber Security Centre (NCSC), the Digital Trust Centre (DTC) & CSIRT-DSP. However, it will be necessary to put additional governance measures in place for the other stakeholders, including the **creation of a strategic governance board and an agenda board.** The latter must determine which joint, substantive products the analysis and resilience centre will develop.

When building the trusted community, clear criteria must be formulated for participation in the Cyclotron platform. These criteria should focus primarily on a good definition of the term 'maturity', which requires further development. The researchers take the first step towards this in this report. To build trust successfully, it will also be necessary to integrate various safeguards, particularly safeguards relating to the

participation of private organisations. Agreements about confidentiality and rules of conduct will be beneficial too.

The Cyclotron platform will fit in well with existing initiatives in the landscape for information sharing, such as the Cyber Intel/Info Cell (CIIC), the Nationwide Network of Information Exchanges (*Landelijk Dekkend Stelsel van informatieknooppunten*, LDS), the National Detection Network (*Nationaal Detectie Netwerk*, NDN) and SecureNed. The researchers recommend that a **close partnership be developed with the CIIC** and **that the LDS, the NDN (in part) and SecureNed be integrated into the Cyclotron platform in the future**, which will ensure the achievement of more synergy, focus, clarity and central control in the landscape for information sharing.

The creation of the **Cyclotron platform will be a complex process and implementation will need to take place step by step**. The researchers recommend that the design set out in this report be used as a **blueprint for the future**. In the short term, this blueprint can be used to make choices about the aspects to be developed based on legal and practical considerations.

The researchers feel it would be a risk to build the Cyclotron platform as a new initiative in addition to existing initiatives. Therefore, they advise **that development take place as part of one of the existing initiatives. The researchers believe that SecureNed is the best candidate**. It will not be necessary to use Cyclotron as the new name in the landscape. It would be better to use the name SecureNed or to replace the name SecureNed with a name that has a readily identifiable narrative, a strong brand value and broad support.

While conducting the exploratory research, it became clear that there was a **need in the landscape for a good 'target and victim notification' solution**. This was placed outside the scope of the Cyclotron design. The researchers recommend **the development of a separate solution for this subject** – which has a very clearly delineated scope – with the relevant private and public partners.

INTRODUCTION AND PROBLEM DEFINITION

The 2018 Dutch Cybersecurity Agenda² (*Nederlandse Cybersecurity Agenda*, NCSA) included the following goal:

"The national situational assessment will be enhanced through the creation of a cooperation platform with the aim of sharing an armamentarium with interested organisations more quickly and more widely within the legal parameters. Attention should be paid to the requirements in the field of information security. Recipients must be sufficiently mature to facilitate information sharing."

In 2020, the implementation of the above-mentioned action point led to the creation of the CIIC, in which the AIVD, MIVD, NCSC, Public Prosecution Service (*Openbaar Ministerie*) and police have started an extensive exchange of intelligence within the cyber domain.

The next step in the implementation of this action point was to identify possibilities to share information in a broader context with both public and private partners. To that effect, an exploratory research project under the working name 'Cyclotron' was launched in October 2021. This report is the result of this exploratory research, which was conducted by Petra Oldengarm and Lex Mooy.

PROBLEM DEFINITION

The starting point for the Cyclotron exploratory research project was the observation that **an insufficient amount of information is shared by public and private partners when a cyber incident occurs or is imminent**. This information is necessary to be able to increase cyber resilience and to reduce digital threats.

² <https://www.nctv.nl/onderwerpen/nlsa/documenten/publicaties/2018/04/21/nederlandse-cybersecurity-agenda>.

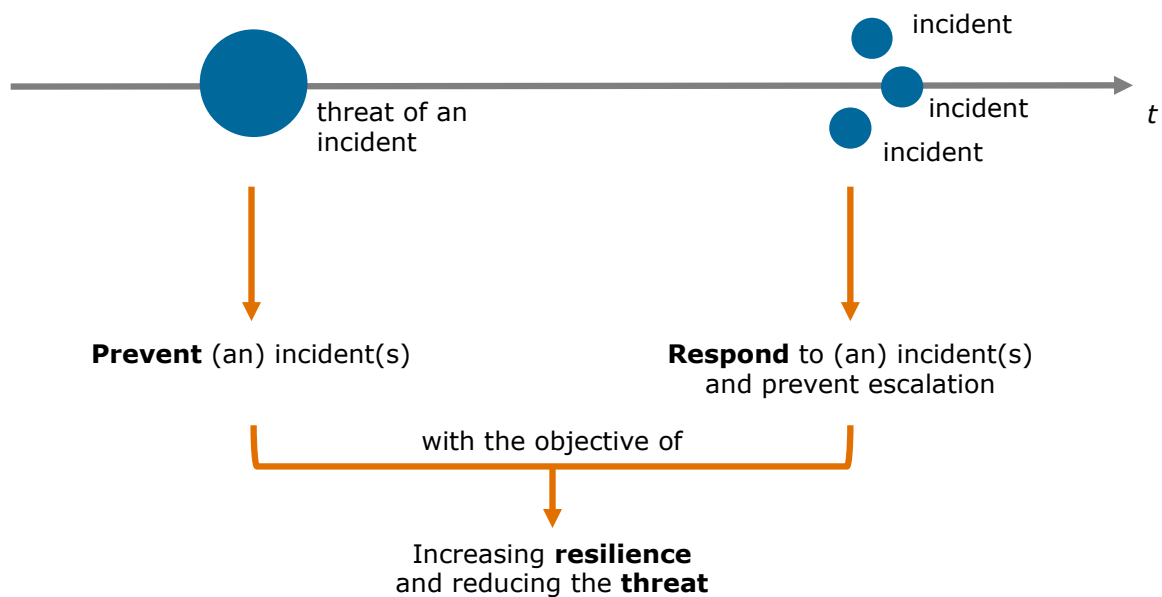


Figure 3 - Public and private parties need information when cyber incidents occur or are imminent

When a cyber incident occurs or is imminent, public and private parties may have relevant operational and tactical information, experience and context. Sharing this information will help address the consequences of cyber incidents more effectively and efficiently, increase cyber resilience and reduce the threat. However, public and private parties currently do not share this information or fail to do so quickly enough.

Furthermore, there are no joint, combined analyses of the available information that could help to achieve a better interpretation of occurring or imminent cyber incidents and possible action frameworks. Finally, after making a choice, parties are too slow to switch to an appropriate action framework. It is often even unclear what would actually be appropriate.

Given the present lack of willingness and absence of possibilities to share information in a broader context, many opportunities that would help increase resilience and reduce the cyber threat remain underutilised.

The research questions explained in the next section of this report were formulated based on the problem definition above.

RESEARCH QUESTIONS AND READING GUIDE

RESEARCH QUESTIONS

The Cyclotron exploratory research project focused on investigating how information about occurring or imminent cyber incidents can be shared more effectively between public and private partners. The main research question was as follows:

What are the possibilities and requirements for strengthening public-private partnerships at an operational and tactical level³ so the response to cyber incidents becomes more effective and efficient?

To answer this question properly, the following research questions were explored in the first phase of the exploratory research project:

1. What does the **current landscape regarding information sharing** look like (public and private), what are its shortcomings and which **needs** should be addressed?
2. Which **potential solutions** exist for information sharing in **other countries and domains** and which lessons could be learnt from these solutions?
3. Will a new cooperation platform help **resolve the underlying problem**?

Because the outcomes of the first phase showed an actual need for increased information sharing between public and private parties, the second phase of the research project saw the development of a design for a possible cooperation platform. The following research questions were addressed:

4. Which **format** would meet the needs of the public and private partners concerned and would build on best practices from other countries and domains?
5. How should a so-called **trusted community** be given shape and which **concrete conditions** will cooperation partners need to meet?

³ The remit for the Cyclotron exploratory research project was explicitly limited to cooperation at the operational and tactical level and excluded cooperation at the strategic level.

6. What are the **required facilities** from a legal, technical, and organisational point of view?
7. How will **the new platform fit in the current and future landscape** for cooperation and information sharing, and how should the connection with other initiatives (like the CIIC) be made?

READING GUIDE

This report sets out the answers to the various research questions. It starts with an analysis of the Dutch landscape for information sharing in the cyber domain and the lessons that could be learnt from initiatives in other countries and domains. Based on the above, the researchers identified needs which – in turn – formed the basis for the design of the platform.

Next, the report looks at the most important elements of the design: the information to be shared, the stakeholders involved and the channels necessary for information sharing. The relevant requirements are discussed as well. Several of these requirements have been investigated in more detail and are explained in more depth in a separate section.

One important next step is to add the new design to the existing landscape, to consider where it would fit in and where opportunities and risks lie for the successful creation of the new platform.

The report ends with recommendations on the creation and implementation of the platform in the near future.

THE CURRENT LANDSCAPE FOR INFORMATION SHARING

Given the long-standing need to share information in the cyber domain, there are already many initiatives to share information in the public domain, the private domain and the public-private domain. There are various national partnerships in other countries as well. Lessons could also be learnt from initiatives outside the cyber domain in which information is already shared intensively. This section sets out the most important findings about the current landscape.

THE DUTCH LANDSCAPE FOR SHARING INFORMATION ABOUT CYBER INCIDENTS

When exploring the current landscape for information sharing, it soon became evident that there is no clear overview of existing initiatives. In December 2020, the Anti Abuse Network⁴ (AAN) put together an initial overview for the domain of abuse information with the so-called 'underground map' (*Metrokaart*).⁵ This map primarily shows that information sharing in the cyber domain is complex, that many parties are involved – from both the public and private sector – and that they often have a number of different roles (for example, as a source, a sharer of information or a recipient of information). Using the underground map, however, it is difficult to gain a good insight into the needs and bottlenecks in the current landscape. Also, the underground map covers just a limited part of the domain that is relevant for this exploratory research project.

⁴ <https://www.abuse.nl>

⁵ <https://www.abuse.nl/publicaties/metrokaart-december-2020.html>

For this reason, the Cyclotron exploratory research team developed a model⁶ that shows the landscape in a manner that makes it possible to compare the various initiatives with each other better.

In this model, the initiatives are compared on the basis of the following three aspects:

1. Information. The different types of information and which information is shared within the initiative.
2. Stakeholders. The stakeholders that are active in a network, the role they play and how information flows between them.
3. Channels. The types of communication channels being used to share information.

Figure 4 visualises the connections between the three aspects above.

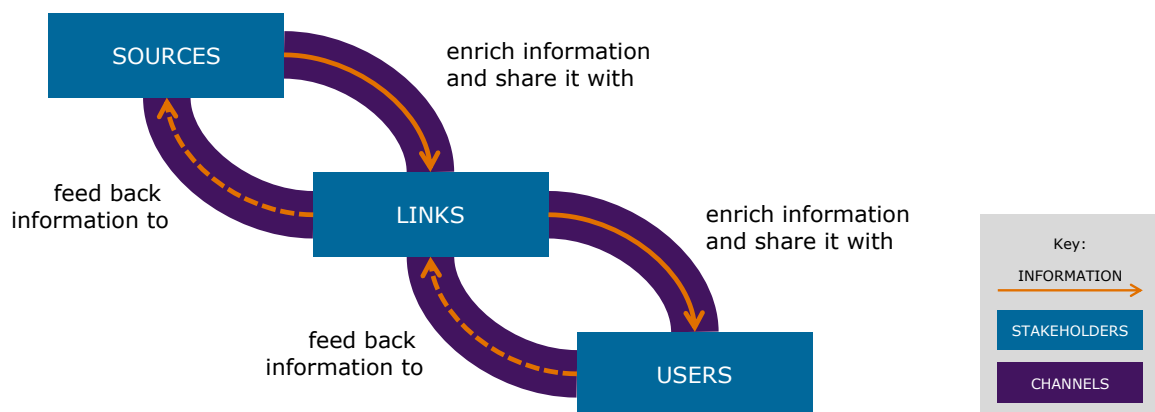


Figure 4 – The connections between information, stakeholders and channels

For the purpose of this exploratory research, cooperation initiatives that are currently active in the landscape were included. These involve a number of public and/or private stakeholders. The information sharing tasks of individual organisations such as the NCSC and the DTC and policy-related and strategic, permanent forms of consultation (such as the directors’ consultation on cybersecurity (*Directeuren Overleg Cybersecurity*)) were excluded from the analysis.

In addition, there are various initiatives under construction, such as the Government SOC System Enhancement Programme (*Versterken SOC Stelsel Rijk, VSSR*) (public), the NL CISO Circle of Trust (private) and the Dutch Security Hotline (*Nederlands Security Meldpunt*) (private). The researchers spoke to the representatives of these initiatives and included the gist of their input in this final report. Only the input of the Dutch Security Hotline was represented in the model (to a limited extent).

The following initiatives were explored in-depth in the context of Cyclotron (see Figure 5):

- CIIC

⁶ This model was developed with the input of Prof.dr. B. van den Berg of Leiden University.

- Nationwide Network of Information Exchanges (LDS)
- National Detection Network (NDN)
- SecureNed
- Information Sharing and Analysis Centres (ISACs)
- Dutch Security Hotline

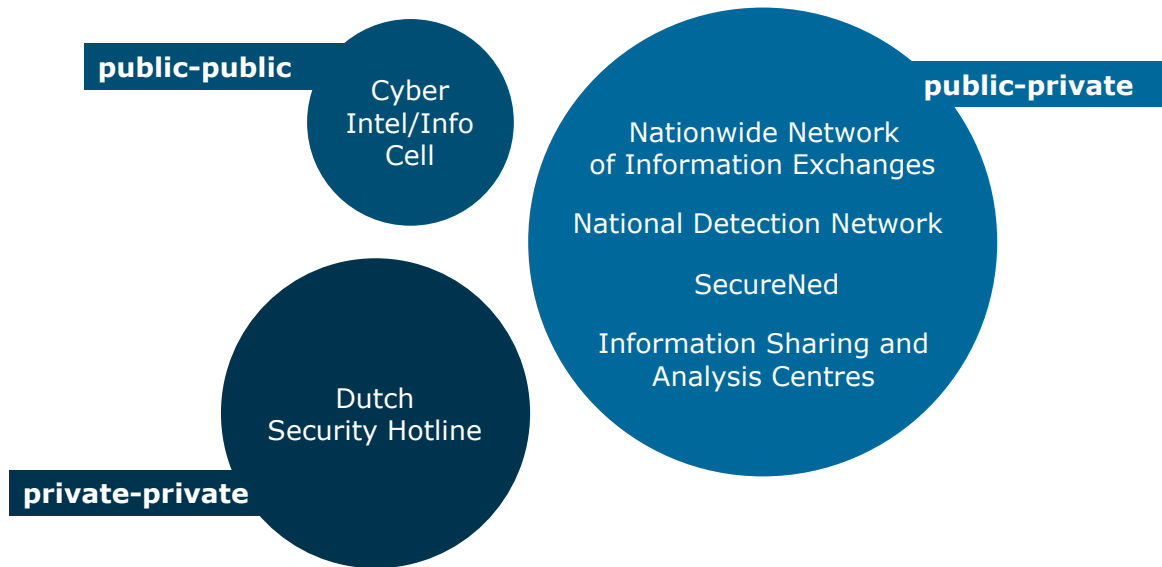


Figure 5 - Initiatives explored in-depth in the context of Cyclotron

With Cyclotron in mind, the researchers spoke to representatives of the initiatives in question and then drew conclusions about needs and bottlenecks with respect to information, information sharing, stakeholders and channels. These are explained in more detail in the paragraphs below.

Information-related needs and bottlenecks

The term 'information sharing' suggests a clear definition and demarcation of the word 'information'. However, the exploratory research showed that the various initiatives share a wealth of information. Figure 6 shows that two types of information are shared:

1. Raw data. Raw data is defined as data that is compared without being subject to any further, extensive analysis. This type of data is often of an operational nature – for example, information about vulnerabilities or attackers.
2. Analysed information. This type of data is often more tactical or strategic in nature and ensues from further analyses of raw data – for example, phenomenon analyses and best practices.

Information can also be placed on a timeline. In other words, some information relates to the past – for example, historical analyses and registers containing information about incidents – while other information relates to the present and current events. Finally, other information sets the direction for the future – for example, trends and predictions.

For extensive background information about the modelling above, see page 55 and onwards of the annexes. The information model is visualised in Figure 6.

To be able to use the information model in practice, several other dimensions of information are relevant and were included in the exploratory research too:

- Implementation level. The implementation level can be broken down into operational, tactical and strategic aspects. The aspect applicable depends on the need of the information user.
- Confidentiality. Various classifications are used to express the confidentiality of information. For example, some information is public, other information may not be shared outside the organisation, while other information is subject to government classifications such as 'restricted' or even 'state secret' ('confidential', 'secret' or 'top secret').
- Shareability. If information is shared, it will be relevant for the recipient to know how the information is to be handled. The sender can specify this by using the Traffic Light Protocol⁷ (TLP).

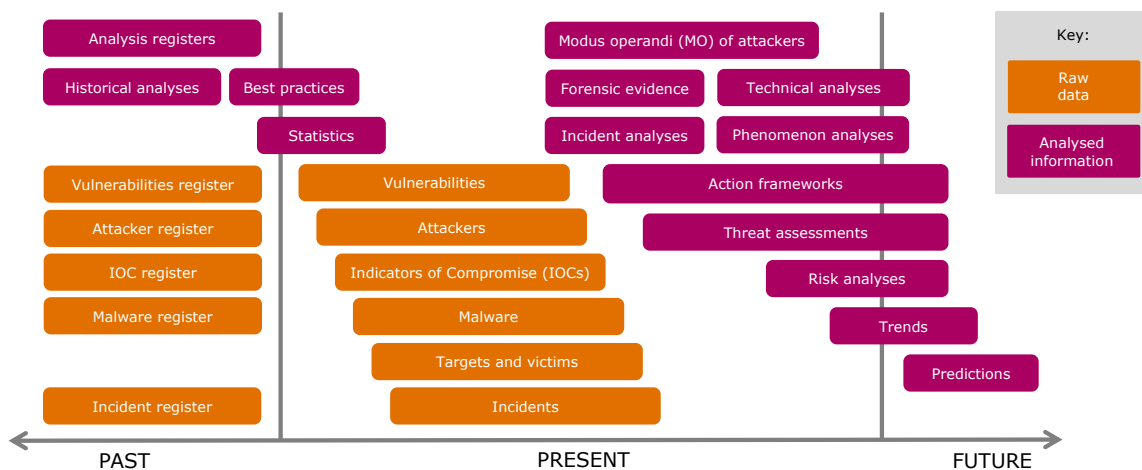


Figure 6 – Information model

Each of the initiatives explored has been plotted onto the information model described above. For more information, see page 58 and onwards of the annexes. Based on this modelling and exploratory meetings with representatives of these initiatives, the researchers arrived at a number of general conclusions about needs and issues in the field of information.

The most important conclusions⁸ with regard to information are as follows:

- 1. Although a wealth of operational, raw data is shared, this happens in a fragmented way in many different networks.**

⁷ <https://www.ncsc.nl/onderwerpen/traffic-light-protocol>

⁸ Some conclusions extend beyond the scope of the Cyclotron project, but have been included anyway.

2. **Indicators of compromise (IOCs) are shared regularly but are still only being developed jointly to a limited extent.**
3. **Tactical and strategic information is not yet analysed jointly to a sufficient degree.**
4. **Parts of the information landscape – for example, the registration of incidents and the performance of historical analyses – are currently being dealt with only cursorily or not at all.**

Stakeholder-related needs and bottlenecks

The sharing of information involves various stakeholders. These may play several roles:

1. Sources. Stakeholders with information that they share with other stakeholders.
2. Links. Stakeholders with a sharing function (hub function) in a network. They sometimes enrich information and then share it with other stakeholders. An example are the so-called OKTTs (organisations that objectively have the task to provide other organisations or the public with threat information), which represent a broader base of clients.
3. Users. Stakeholders that receive information and use it to increase their own resilience or reduce the threat.

One of the reasons for the diffuse nature of the landscape for information sharing is the fact that stakeholders in the landscape sometimes have several roles. For example, links can be the users of information as well. Links sometimes also function as hubs for other links, resulting in a hierarchy of links.

Information flows between the various stakeholders, often from sources to links and from links to users. The opposite is possible as well, but currently happens only to a limited degree in practice.

Figure 7 shows a network of sources, links and users.

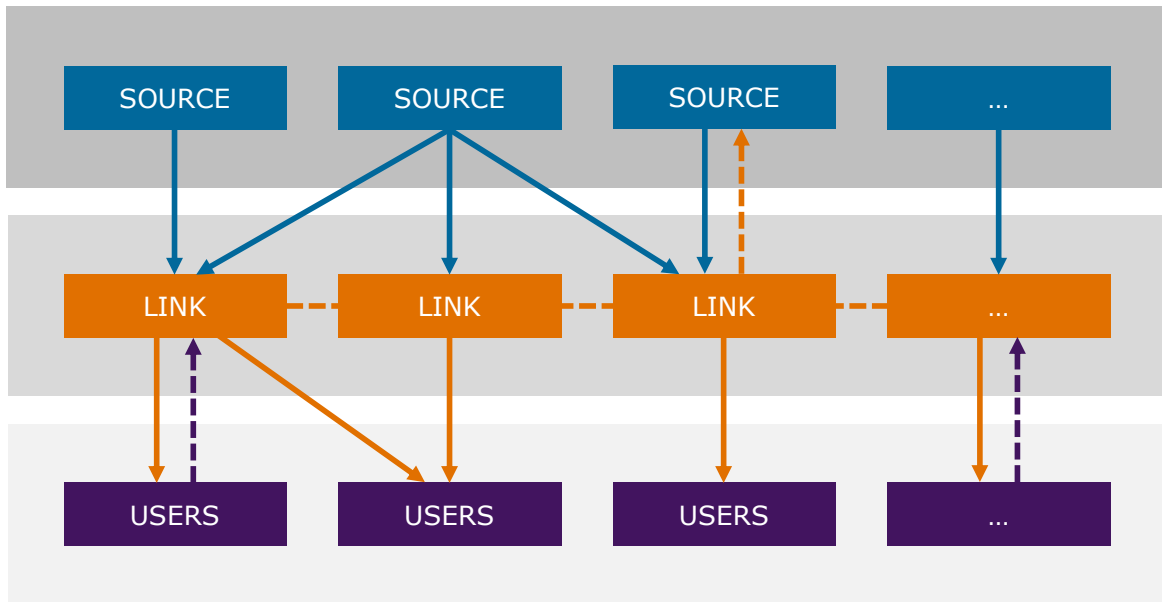


Figure 7 - Connections between stakeholders when sharing information

The researchers identified the network of sources, links and users for each of the initiatives explored. See page 58 and onwards of the annexes for more information. Based on this modelling and meetings with representatives of the initiatives in question, the researchers arrived at a number of general conclusions about needs and issues in the field of stakeholder networks.

The most important conclusions about stakeholders are as follows:

1. **The stakeholder landscape is very diffuse**, at source, link and user level, due to role mixing and differences in maturity.
2. **In the current landscape, the NCSC plays a central role as an important link in many initiatives. However, it does not formally function as a national CSIRT in the Netherlands because of its remit, which has been limited to critical infrastructure protection and central government.**
3. **Each government organisation has its own role and network in the landscape and central control and direction are absent.**
4. **The initiatives currently only reach part of the non-critical business community.** The DTC plays a primary role in efforts to reach this target group.

Channel-related needs and bottlenecks

The information shared between stakeholders finds its way to recipients via channels. Three types of channels are conceivable:

1. Channels that share information with each other on an automated basis and without human intervention (machine-to-machine). For example, interconnected digital systems that forward information on the basis of automatic rules.

2. Channels in which people share information with each other through a technical medium. For example, email, chat channels, systems for the safe sharing of digital files, telephone and video calls and websites that provide information.
3. Channels in which people share information with each other through direct contact. This involves face-to-face contact, for example at a meeting.

The three channels are visualised in the figure below.

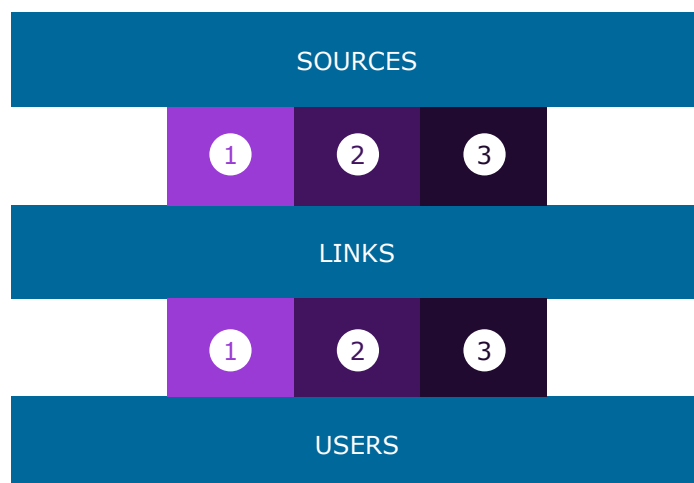


Figure 8 - Different types of channel are possible between sources, links and users

The channels used have been identified for each of the initiatives explored. See page 58 and onwards of the annexes for more information. Because the channels between the links and users are of primary relevance, they were the main focus of the analysis. Based on this modelling and exploratory meetings with representatives of these initiatives, the researchers arrived at a number of general conclusions about needs and bottlenecks where channels are concerned.

The most important conclusions about channels are as follows:

1. **Many different types of channels are being used.**
2. **Few machine-to-machine channels are being used.**
3. **Each information sharing initiative creates its own new channels and there is little overlap.**
4. **Informal channels are important for information sharing and** stem from personal contacts, intrinsic motivation and trust.

General shortcomings and needs

Besides the shortcomings and needs identified on the basis of information, stakeholders and channels, a number of general conclusions can be drawn.

Before formulating these conclusions, it is wise to consider why such a diffuse landscape for information sharing has developed in the Netherlands over the years. It

is important to have some insight into the above because it also impacts the potential success of a new initiative.

Although more in-depth research into these causes could generate even more insight, the researchers see the following **critical success factors** in any event, based on the discussions:

1. **Informal networks are vital** when seeking to develop good partnerships. A solution that focuses on the provision of a good technical channel alone is important, but not sufficient.
2. It is important to recognise that public and private stakeholders have a **significant shared interest**.
3. A **pragmatic start** helps to ensure that the exact specifics of an initiative are concrete and manageable. If there are too many limitations in advance, the transaction costs incurred when developing the solution will be too great for it to be possible to get an initiative off the ground.
4. It is important not to repeat the mistake of positioning a new, extra initiative next to existing initiatives. It is far more important for **consolidation to take place within the landscape**. A new solution in the form of another initiative will cause even more fragmentation and a reluctance among parties to use it.
5. The government can encourage private parties to participate in an initiative by **offering the right incentives**.

Based on the exploratory meetings held as part of the research, various requirements can be formulated for the legal framework, the interests of stakeholders, the development of trust and the practical specifics of, and technology for, a cooperation platform. These are set out in the table below.

Domain	Challenges, needs and requirements
Legal framework	<ul style="list-style-type: none"> • The introduction of the European Directive on Security of Network and Information Systems (NIS2) has led to a lack of clarity about the scope and remit of the NCSC and the DTC and, as such, a lack of clarity about the role that both organisations play in the landscape for information sharing. • The diversity in relevant legislation (for example, the Intelligence and Security Services Act 2017 (<i>Wet op de inlichtingen- en veiligheidsdiensten</i>, Wiv), the Network and Information Systems Security Act (<i>Wet beveiliging netwerk- en informatiesystemen</i>, Wbni) and the Police Data Act (<i>Wet politiegegevens</i>, Wpg)) impedes information sharing across the government and can also cause bottlenecks in collaborative partnerships with private parties. • Private parties encounter legal challenges with respect to privacy (General Data Protection Regulation, GDPR), cartel formation, market disruption and liability.

Trust	<ul style="list-style-type: none"> • There is a need for objective criteria for the admission of partners. • There is a need for the possibility to share highly sensitive information in a very limited group. For example, the General Security Requirements for Defence Contracts (<i>Algemene beveiligingseisen Defensieopdrachten</i>, ABDO) and the General Security Requirements for Central Government Contracts (<i>Algemene beveiligingseisen rijksoverheid</i>, ABRO) could be used as assessment frameworks. • There is a need to choose to share some information in the Netherlands alone. Other information could also be made shareable in a European or worldwide context.
Interests	<ul style="list-style-type: none"> • It is essential for information sharing to be a two-way process. • There is a need among public parties for input from the private sector. • Both public and private parties have a need for more central control of the landscape for information sharing. Private parties mainly look to the government for this. • The security services need stronger connections and a legal framework for their cooperation with other organisations, whether public or private. • The interests of the stakeholders in question must be made explicit. • When sharing information, stakeholders sometimes find this has a negative impact on their own information position. This applies for both public and private parties. • Market parties sometimes have objections to the sharing of information with security companies because of the commercial interests security companies have. • Security services are mainly able to share generic information. There is currently no good, optimal legal format to facilitate the broad sharing of specific information.
Practice	<ul style="list-style-type: none"> • Information sharing can be problematic if users work with suppliers. It is important that suppliers are also viewed as primary users of information. • There is a considerable lack of clarity about the terminology used. The model introduced in Cyclotron could be a step towards the resolution of this problem by giving better insight into exactly which information will be shared. • Various government organisations use similar information, making their exact role unclear for clients. • Victim notification by the government will be difficult to achieve, but is necessary.

	<ul style="list-style-type: none"> • Various threat intel feeds that are received centrally are only shared with a select group and only to a limited extent. • Action frameworks must be adjusted to reflect a specific context and the maturity level of the recipient. • Economic security is seen as an important new theme that is relevant in the context of information sharing. • Mature organisations want to obtain raw data more quickly, because they are able to interpret it themselves. • Conversely, immature organisations want more interpretation and a clear action framework tailored to their particular sectors. • There is a need for the performance of more joint tactical analyses. • The police would like to be able to share information about victims better. • There is a need to receive more reports about incidents (not only through reports filed with the police, but also from a broader range of sources) to gain better insight into the nature and extent of incidents.
Technology	<ul style="list-style-type: none"> • There is a need for more machine-to-machine communication. • The consolidation or standardisation of channels in the landscape will create efficiency and an overview.

Table 1 - Overview of general challenges, needs and requirements

INTERNATIONAL INITIATIVES

Various international initiatives were studied to ascertain the extent to which they reflect needs and bottlenecks in the Dutch cyber landscape. Initiatives in a number of countries were considered in more depth: France (ANSSI & Cyber Campus), the United Kingdom, Canada and Denmark.⁹

At a general level, it is good to point out that some other countries have initiatives that are comparable in part to those we already have in the Netherlands. Various countries have networks in which threats and risks are discussed in a manner similar to the way in which ISACs are organised in the Netherlands. Sometimes, networks similar to the LDS and the NDN in the Netherlands have been created to share operational and tactical threat information. For as much as the exploratory research has been able to ascertain, these initiatives do not go much further than what is already being done in the Netherlands.

However, there are three positive exceptions:

⁹ These countries were chosen based on meetings with participants from the SOC and several stakeholders.

1. The Cyber Campus in France. A large project in which organisations have been physically brought together in a luxury new building in the business district of La Défense in Paris. With the support of President Macron, the object of the project is to reap the rewards of cooperation. The French approach to this complex project is impressive. The new building is now in use and nearly all its spaces have already been leased out. It still remains to be seen whether this concept will actually result in the envisaged cooperation, but the solid foundations are there. The project has gained the broad commitment of many organisations in the public and private domains.
2. The CISP platform in the United Kingdom. This large distribution platform is interesting because it enables the NCSC-UK to reach a broad audience with the information published.
3. The i100 programme in the United Kingdom. In this programme, the NCSC-UK works closely with approximately 25 industrial partners (the ambition is to increase this number to 100 in the future) that second employees to the NCSC-UK on a part-time basis to share information on a demand-driven basis. The private sector benefits from positioning employees close to the NCSC-UK.

The most important lessons that could be learnt from the foreign initiatives above have been incorporated into the Cyclotron design. The other lessons for Cyclotron are summarised below per country/initiative.

Country – initiative	The most important lessons
Canada – CCCS	<ul style="list-style-type: none"> • CCCS has a portal that users can log into to indicate their information need.
Denmark – CFCS	<ul style="list-style-type: none"> • No specific lessons.
France – ANSSI	<ul style="list-style-type: none"> • ANSSI works closely with cybersecurity companies. Since 2014, ANSSI has been certifying these companies and using them to improve the resilience of the critical infrastructure and also provide incident response services.
France – Cyber Campus	<ul style="list-style-type: none"> • The pragmatic French approach: organise cooperation by bringing all the parties together. • A wide range of organisations come together on the Cyber Campus: large, small, public, private, national and international. • Various subjects are discussed in the cooperation spaces (Commons). The choice of subject depends on current events and/or needs. • Innovation is an important subject, as are current cyber subjects such as AI and crypto. • A great deal of attention is paid to education, attracting new talent and encouraging diversity. • The Campus has the ambition to cooperate actively with other parties at an international level (in Europe in particular).

The United Kingdom – CISP	<ul style="list-style-type: none"> • A digital distribution platform can be a powerful tool when seeking to reach a broad target audience. • However, if the community gets too large, this could reduce the level of trust experienced and, as such, have a negative impact on information sharing (reciprocity).
The United Kingdom – i100 programme	<ul style="list-style-type: none"> • There is an effective trusted community. A structured process is in place with the capacity required to ensure information sharing by the NSCS-UK. • Within the i100 programme, a high degree of confidentiality has been achieved through a system of affiliates per organisation. • The commitment level is high because the individuals active in the i100 programme for private companies have applied for the role themselves.

See the annexes, from page 70 onwards, for a more comprehensive report on these foreign initiatives.

NATIONAL INITIATIVES IN OTHER DOMAINS

Three national initiatives were studied to ascertain the extent to which lessons could be learnt from them for Cyclotron. These were the following:

1. The Counterterrorism (CT) Infobox. This is a cooperative platform of various public organisations and resides under the AIVD. The object of the CT Infobox is to contribute to the fight against terrorism.
2. The Electronic Crimes Task Force (ECTF). This alliance focuses on addressing digital crime, primarily in the financial sector. Four major banks, a credit card provider, the Public Prosecution Service and the police are part of the alliance. The object of the ECTF is to address digital crime and fraud (phishing is an important theme at the moment).
3. The 10 regional information and expertise centres (RIECs) and the National Information and Expertise Centre (Landelijk Informatie- en Expertise Centrum, LIEC). The RIECs and the LIEC focus on addressing subversive crime. They connect information, expertise and strengths from different government agencies. The RIECs and the LIEC also stimulate and support public-private partnerships in tackling subversion.

At a general level, it is good to point out that all the initiatives come up against more or less the same legal restrictions. These pertain primarily to the sharing of personal data without legal grounds (in the case of the ECTF and the RIEC-LIEC). Domestic legislation also places restrictions on sharing information with parties that do not fall within the scope of the legislation in question. Besides this, several lessons could also be learnt with respect to cooperation agreements, governance, and communication.

Initiative	The most important lessons
CT Infobox	<ul style="list-style-type: none"> • Legal safeguards are very important. • Rapid decision-making by means of an efficient governance structure is vital. • The action framework and IOCs often constitute the most important need for recipients. The reason for this need is less important. • Information shared externally cannot be traced back to the source organisation.
ECTF	<ul style="list-style-type: none"> • The use of a covenant in the absence of a legal mandate needs to be avoided. • The inability to share certain personal data is causing serious operational inefficiency. • Due to the restrictions imposed by the GDPR, efforts focus primarily on sharing information about the modus operandi. • All participating parties supply a minimum of 1 FTE. The lead organisation (the police) provides the highest number of FTEs. • Any of the participating parties can initiate an investigation. • Each participating party has a representative at the tactical/strategic level (the supervisory committee). This committee also determines the themes. • Consideration is given to the question of 'what constitutes a report?', which makes it easier to share information. • Banks have agreed never to compete over security.
RIEC and LIEC	<ul style="list-style-type: none"> • Due to the absence of legal grounds, restrictions apply when sharing information. • However, there is a covenant and a privacy protocol. • This initiative facilitates communication toolkits and clear action frameworks that meet the needs that users have. • To determine a strategy, information will be brought together in a strategic knowledge centre that is still to be created. • Public parties are cautious about sharing information with private parties in the future (not yet part of this initiative).

See the annexes, from page 74 onwards, for a more comprehensive report on these domestic initiatives.

MORE INTENSIVE INFORMATION SHARING NEEDED

The exploratory research conducted on national and international initiatives for information sharing shows that parties are already cooperating in many areas. Over the years, a diffuse landscape for information sharing in the cyber domain has developed in the Netherlands. In this landscape, a new demand has arisen for

further-reaching information sharing, as well as a need for the consolidation of initiatives in the landscape in order to achieve more overview and control.

At the international level, it should be noted that information sharing in the cyber domain is currently high on the agenda in many countries. In the countries studied, there are initiatives that go beyond what is currently happening in the Dutch landscape, but only to a limited degree. However, there were several occasions when the researchers were asked to join forces internationally and research the extent to which European or global networks could be built (or extended) to make it possible to share information more widely.

While studying national initiatives, the researchers learned that information is shared successfully in other areas as well, although this has been delayed in recent years due to the far-reaching provisions of the GDPR. Because confidential personal data is processed as part of most collaborative partnerships in other domains and information sharing is subject to restrictions in this field, the legal context for the processing of personal data about cyber incidents requires extra attention.

Based on the exploratory research conducted on the national and international landscapes for information sharing, the researchers conclude overall that there is an **urgent need to share information with regard to occurring or imminent cyber incidents more intensively**. When sharing information, a stakeholder network consisting of both public and private parties is important. In the first phase of the exploratory research, the researchers formulated a large number of needs, challenges and requirements to be taken into consideration when developing a platform. The above provided important input for the design phase of the Cyclotron project, the result of which follows in the next section of this report.

DESIGN OF THE CYCLOTRON PLATFORM

Based on the exploratory research conducted with regard to the landscape for information sharing, the researchers observe that the platform needed is one in which information is shared between public and private parties more intensively than is currently the case. Information sharing should focus on the following common objective:

To make the Netherlands an unattractive target for digital attacks

Various organisations actively strive to achieve the objective above, some in the public sector and others in the private sector or in academia. Some are motivated by an individual interest, some by a broad social interest, some by addressing digital attacks and others by working towards increased resilience.

However, what all these organisations have in common is a broad need for information. The researchers envisage that the Cyclotron platform will meet this need.

INFORMATION NEEDS AND OBJECTIVES

The starting point for the design is the observation that the information needs users have are directly proportional to their maturity. The following two needs emerged from the analysis of the landscape (see Figure 9):

1. High-maturity organisations need to receive unanalysed raw data quickly. They say that speed is of the essence where this type of data is concerned. They want to embed the data received within the context of their own organisation and connect it with other information, which will enable them to take prompt action.

2. All organisations need analysed information. The analyses in question could be carried out jointly.

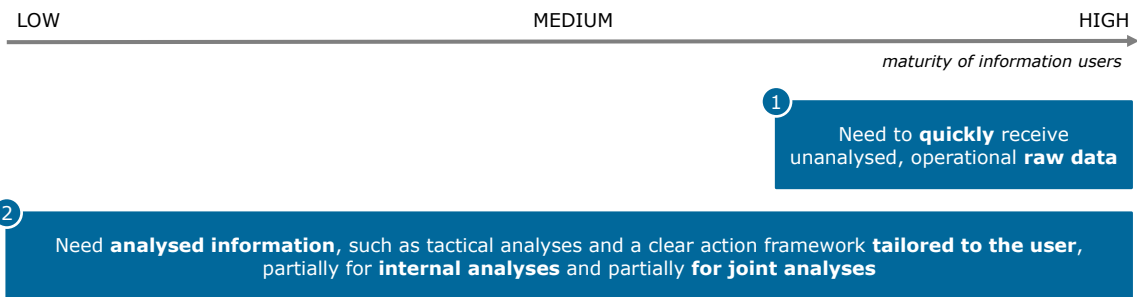


Figure 9 - Two information needs in the context of Cyclotron

These information needs can then be translated into three purposes for information sharing (see Figure 10):

1. To share raw data quickly (push). In this case, organisations share their relevant raw data with organisations affiliated with the network as quickly as possible.
2. To request information (pull). Sometimes, organisations want to approach parties affiliated with the network with a question about specific information they need (both raw data and analysed information). The organisations that answer may choose to send their answers to the requesting organisation alone or to other affiliated organisations as well.
3. To analyse information together. In this case, organisations bring together information about a certain subject. By deploying their expertise together, they can draw new conclusions that can then be shared more broadly.

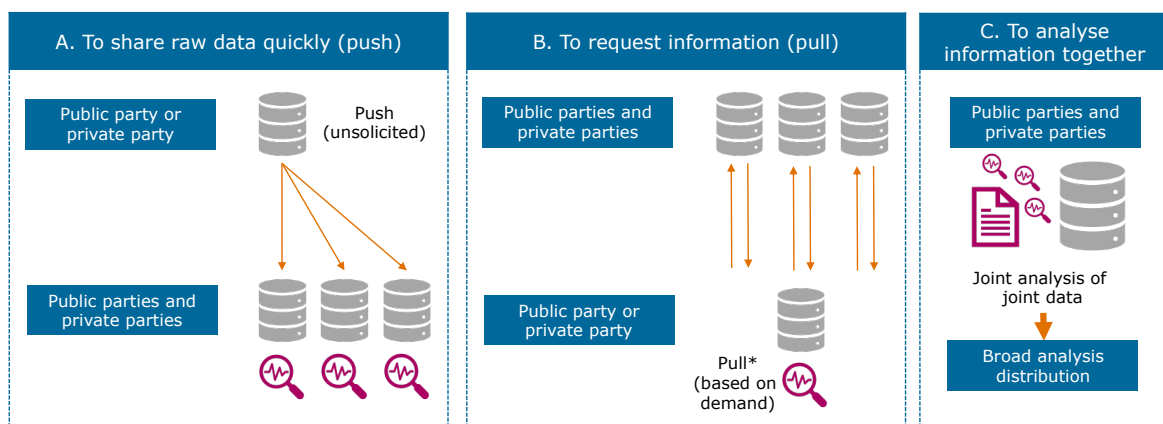


Figure 10 - Three purposes for the Cyclotron platform

The researchers based the design for the Cyclotron platform on the two information needs in Figure 9 and the three purposes in Figure 10, which were developed in more detail.

DESIGN METHOD

The model described in the previous section was used when putting together a design for the Cyclotron platform. The design includes the *information* to be shared, the *stakeholders* involved, how stakeholders are to cooperate with each other and the *channels* needed for information sharing purposes. The requirements that need to be met to ensure that the Cyclotron platform is effective were investigated for each of these elements (see Figure 11).

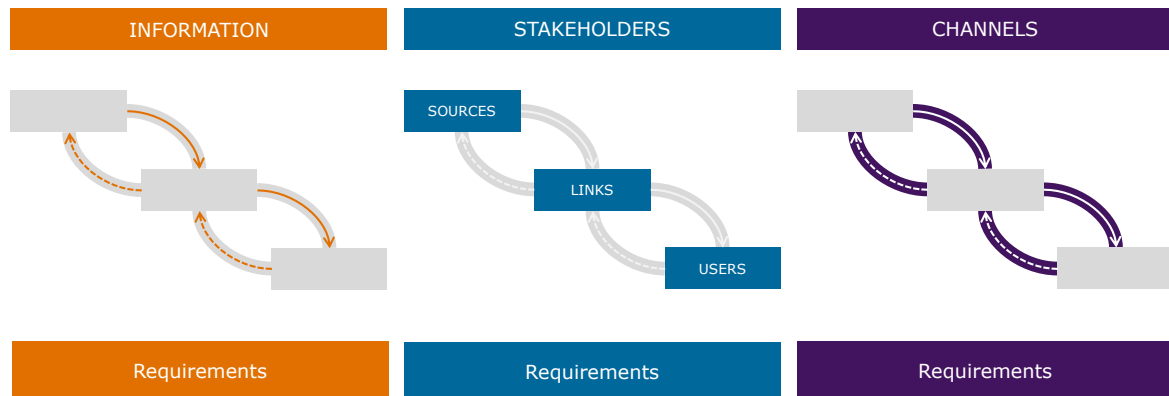


Figure 11 - Design method: information, stakeholders and channels

Because the design method is based on the model previously developed to analyse the landscape, it will be possible to ensure that the platform fits in the landscape well. This is explained in greater detail in the paragraph entitled *Alignment with the existing landscape*, from page 46 onwards.

During the design process, a number of sessions were organised for a big group of stakeholders from the public and private sector to seek their input. The resulting information was supplemented by input from the academic domain (see the annex on page 70). The input from these sessions was incorporated into the design, which is explained in more detail in the paragraphs below.

The design developed in this section is a blueprint for the years ahead. It must be regarded as the roadmap for the next five years. Choices will need to be made during the step-by-step implementation of the design. The recommendation of the researchers in this respect is set out on page 52.

DESIGN: INFORMATION

The needs identified for various stakeholders include a wide need to share information for the three purposes named above: to share raw data quickly, to request information and to analyse information together. The table below shows the need for information for each purpose, which is visualised in Figure 12.

To share raw data quickly (push)	To request information (pull)	To analyse information together
Vulnerabilities IOCs Characteristics of attackers (bitcoin, attacker profile etc.) Target and victim data Malware Incident information <ul style="list-style-type: none"> - Information about affected systems (relevant log data, architecture information, machine data (OT) and network flows) - Incident analysis Register of incidents from the past to interpret situations in the present	Both raw data from A and analysed data from B	IOCs The MO of attackers Best practices Statistics Incident analyses Phenomenon analyses Action frameworks Threat assessments (limited to e.g. a sector or a current development)

Table 2 – Overview of information needs on the Cyclotron platform

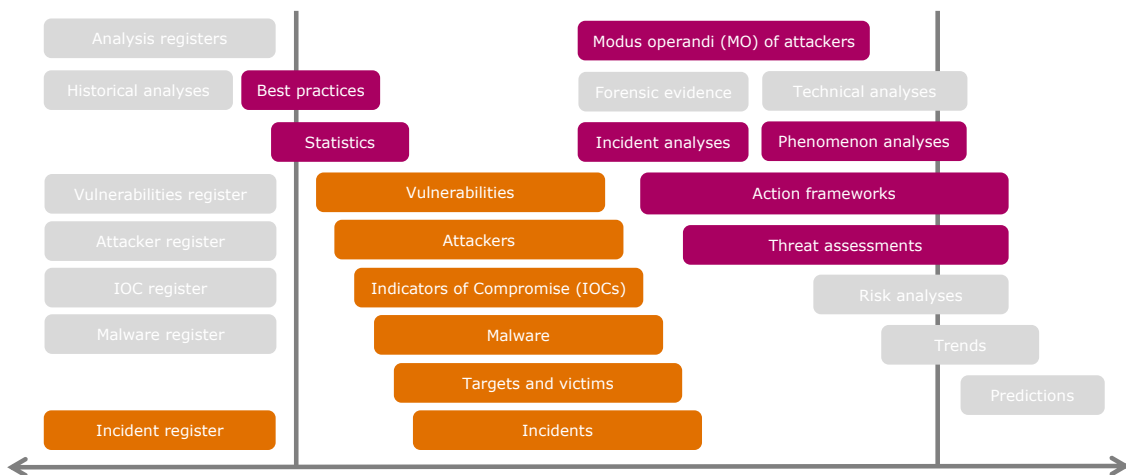


Figure 12 - Selection of information to be shared

All the identified needs were incorporated into the design for the Cyclotron platform, with the exception of so-called target and victim notification. The latter involves the sharing of information about vulnerable systems that may be affected by attacks (targets) or have already been compromised (victims). Although target and victim notification are vital and there is currently a gap in the landscape in this respect, this form of information sharing was not included in the further design of the Cyclotron platform because it does not align neatly with it. The reason for this is explained in

more detail in the *Design a separate solution for target and victim notification* recommendation on page 53.

Various requirements need to be met for information sharing. These are listed in the table below.

Subject	Requirement
Anonymisation	There is a need to share both non-anonymised and anonymised information (note that anonymisation refers to both the information itself and to the source of the information).
Purpose limitation	Owners of information sometimes need to stay in control of the purposes for which users are permitted to use their information. Steps need to be taken to ascertain whether the TLP coding is adequate for this purpose.
Format	It is important to ensure that there is clear agreement in advance on how data is to be structured, making it more suitable for unambiguous use and analysis. Where the format is concerned, the researchers recommend that alignment be sought with international standards.
Legal framework	A clear legal framework should be established for the sharing of data – see page 35.
Quality	When sharing raw data, it is important to indicate the quality of the data so that recipients are able to assess how to use it. If international standards already exist for this purpose, it would be wise to align with them.
Implementation level	The platform will focus on sharing operational and tactical information, not strategic information.
Confidentiality	There is a need to share confidential information, perhaps even at state secret level. To facilitate this, extra safeguards must be built in with regard to the stakeholders permitted to process information of this nature. This has been explained in more detail in the Design: stakeholders on page 28.

Table 3 – Requirements to be met by information in the Cyclotron platform

DESIGN: STAKEHOLDERS

The second part of the design for the platform relates to the stakeholders involved in the sharing of information and how they will be able to work together. The three purposes in Figure 10 (to share raw data quickly, to request information and to analyse information together) can be translated into two information flows in the platform:

1. The (prompt) sharing of operational information between high-maturity stakeholders, both proactively (push) and when asked to do so (pull). The stakeholders in this flow form a network of high-maturity organisations that are both sources and users.
2. The joint analysis of information, development of resilience products and their distribution in the landscape as a whole. In this flow, high-maturity organisations come together to work on specific analyses or products. The next step is to reach users through a network of distribution channels.

The above is visualised in detail in Figure 13. The design for both flows is explained in more detail in the paragraphs below.

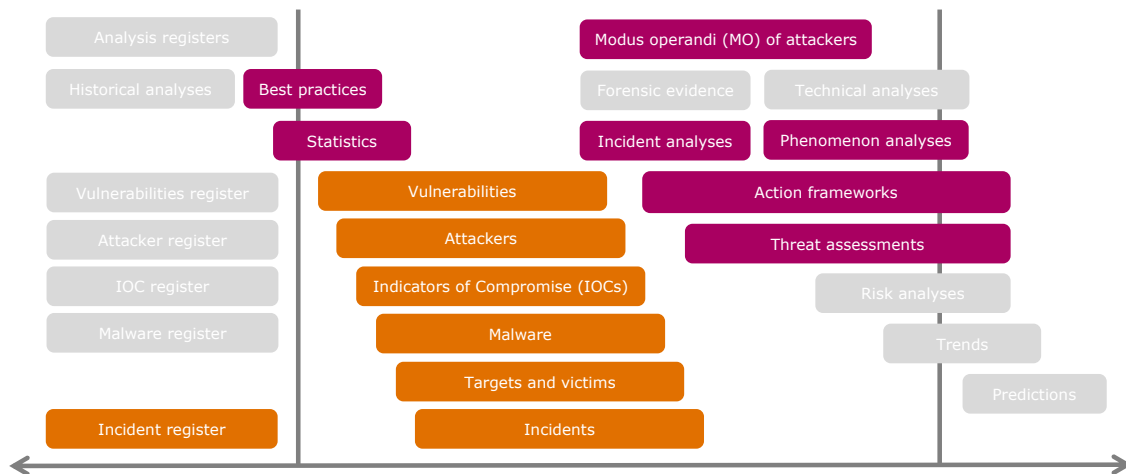


Figure 13 - Stakeholder design, Cyclotron platform

Sharing operational information quickly

A network of high-maturity stakeholders needs to be developed for this part of the design, which is shown on the right in Figure 13. Examples:

- Government organisations, including the police, Public Prosecution Service, NCSC, AIVD and MIVD at the very least
- Cybersecurity companies with relevant information
- Internet service providers and IT managed service providers that monitor information on behalf of their clients
- CERTs and CSIRTs
- OKTT intermediary organisations
- Organisations with the technical capacity to share and receive/process relevant information

The organisations above need to be able to connect to a technical channel to share information. The various requirements need to be met as well. This role was allocated to the information sharing centre, as visualised in Figure 13. It is expressly not the intention for all information to be stored in one central location before being shared further. Instead, the intention is for organisations to be able to connect to a communication channel, after which they will be able to share information directly and proactively (push) with other organisations and also approach these other organisations if they need information themselves (pull). The sender can make the response to a request available exclusively to the requesting party but could also open it up to a number of other parties in the network should it wish to do so.

The information sharing centre is actually a facilitator that ensures the necessary channels are made available and maintained and monitors the requirements applicable to the information and participation.

Creating subgroups with specific requirements for shareability

In the information sharing centre, it is important that parties can choose not to share certain information with stakeholders across the board but to restrict access to it to a limited group. This might be necessary, for example, if highly confidential information is shared and it is important that extra safeguards for the processing of this information are in place on the receiving side (screened employees and limited accessibility for employees of the receiving organisation, etc.). Another example is a situation in which a private organisation wants to share commercially sensitive information with government organisations but not with commercial security companies. A third example is a situation in which a sender wants safeguards that ensure information is only used for Dutch interests. In conclusion, it must be possible to:

1. define subgroups in which specific information can be shared. Objective criteria must dictate which parties are permitted to form part of a subgroup, bearing legal frameworks in mind (such as those relating to the disruption of market forces);
2. specify special requirements that ensure appropriate safeguards are in place when sharing information in a subgroup.

The information sharing centre is responsible for managing these subgroups and developing and safeguarding these requirements. Figure 14 shows a fictitious situation with subgroups. It would be preferable to limit the number of subgroups as much as possible and, as such, only to form a subgroup if strictly necessary and legitimate. If there is a proliferation of subgroups, there is a risk that confidence in the platform as a whole will decrease, and the information flow dry up as a result. Therefore, transparency about subgroups (objective and requirements) is essential.

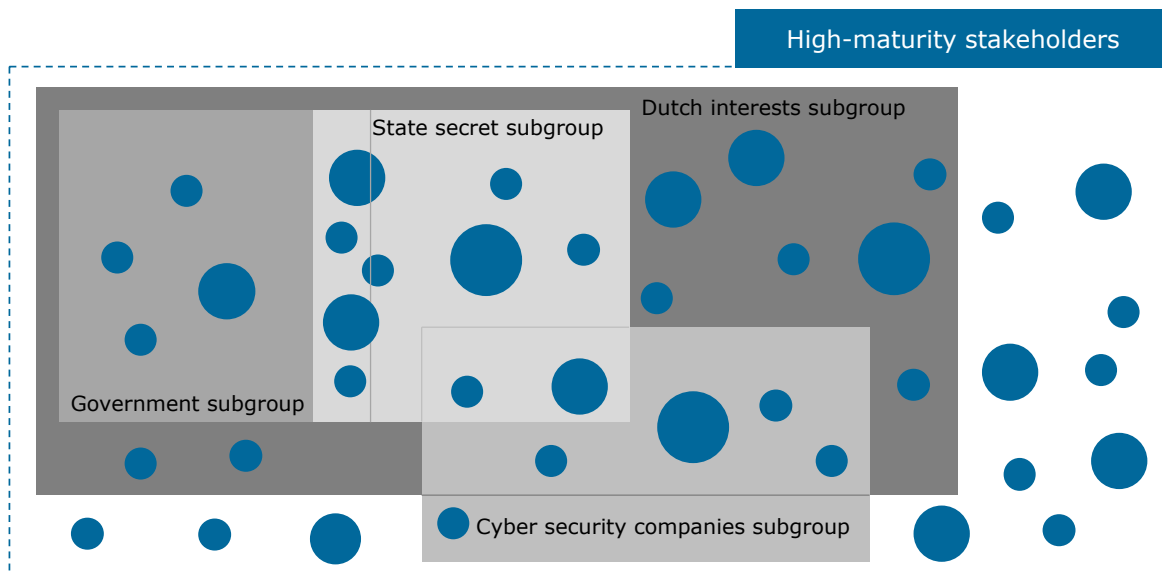


Figure 14 - Possibility to create subgroups with additional requirements

Incident register

The information sharing centre will also be responsible for establishing and maintaining an incident register. Initially, this could be a 'hit-no hit' register that stakeholders can approach to be put in contact with each other if information is available. It is conceivable that the scope of a register of this nature could be broadened in the future. For example, it could also be used to perform phenomenon analyses. The register will then need to be refined.

Requirements for the information sharing centre

The key requirements for the information sharing centre have been elaborated in the table below.

Subject	Requirement
Criteria	Objective criteria are needed to determine which stakeholders will be allowed to participate – see page 43.
Rules of conduct	Rules of conduct must be defined for participation – for example, the answer to the question of how to proceed if a participant is not able to reciprocate.
Reciprocity	Under the push and pull model, parties that want to receive information will be expected to share information as well. Also see <i>Rules of conduct</i> .

Table 4 - Requirements for the information sharing centre

Joint analysis and the subsequent distribution of information

This part of the design, which is shown in Figure 13, involves the following two elements:

1. An analysis and resilience centre. Joint analyses are performed by an analysis and resilience centre with a number of functionalities:
 - a. *Agenda setting*. An agenda for the products created by this centre (such as phenomenon analyses and best practices) will need to be established together with the relevant stakeholders.
 - b. *Stakeholder selection*. An ad hoc partnership will need to be created for each of the activities and consist of experts from the community of high-maturity stakeholders (see the previous paragraph) plus other experts, such as academics.
 - c. *Task implementation*. For each task on the agenda, the ad hoc partnership will be activated to develop the planned product. The appropriate input will be gathered jointly. This could be obtained by various means, e.g. through the information sharing centre, on the basis of requests that have been issued (pull) or by consulting the incident register.
2. A communication and distribution centre. This centre has two tasks:
 - a. Communication. This task involves the determination of the target groups to which specific output from the analysis and resilience centre will be sent. Where necessary, the content and format used will be tailored to the recipient in question.
 - b. Distribution. The core task of the distribution centre is to ensure that specific information reaches the appropriate users. Because it would not be efficient to reach each user directly, it is important to use intermediary organisations for this purpose. Government linking organisations include the NCSC and the DTC, but intermediary organisations are important too (OKTTs, for example). It is also necessary to reach the group of companies to which organisations have outsourced responsibility for a secure IT infrastructure. These organisations are collectively known as *problem solvers*. They include internet service providers (ISPs), IT managed service providers (MSPs) and managed security service providers (MSSPs).

As is clear from Table 5 below, one specific requirement is important for this part of the design.

Subject	Requirement
Capacity	Participants in the analysis and resilience centre must have the expertise necessary to be able to contribute effectively and also be able to make enough time available for participation.

Table 5 - Requirements for the analysis and resilience centre

General requirements for stakeholders

Table 6 provides an overview of the relevant requirements that need to be met for the platform as a whole. It should be noted that there are strong links between the information sharing centre and the analysis and resilience centre. The stakeholders in both centres are highly mature organisations. It is important to support the informal network of which these stakeholders are a part actively, because it is an important basis for trust and the development and expansion of a trusted community. This aspect is explained further in *Building a trusted community* on page 43.

Subject	Requirement
Governance	A governance structure with clear overall control will need to be created, e.g. to set the agenda for the analysis centre and monitor the quality of input and output. Governance must be organised at three levels: strategic (making choices about the direction to be taken by the platform), tactical (setting the agenda) and operational (task performance). See page 40.
Informal network	Many contacts and a lot of trust can be gained through frequent informal contact, which is why sufficient support for this informal network from the platform will be vital. See page 43.
Legal framework	It will be important to have or develop a joint legal framework to facilitate a type of cooperation in which the legal frameworks of the individual organisations are taken into account. See page 35.
Trust	The starting points for trust must be defined in terms that are as specific as possible. For example, allowance must be made for the participation of organisations with an international aspect. See page 43.
Maturity	It will be necessary for clear criteria to be developed with respect to maturity: when will an organisation be considered a low, medium or high-maturity organisation? See page 43.

Table 6 - General requirements for stakeholders

DESIGN: CHANNELS

It is anticipated that a number of channels may be necessary to create the Cyclotron platform (see Figure 15). It is of note in this respect that the channels needed for the information sharing centre and the analysis and resilience centre are the same. A separate channel will be required for the communication and distribution centre.

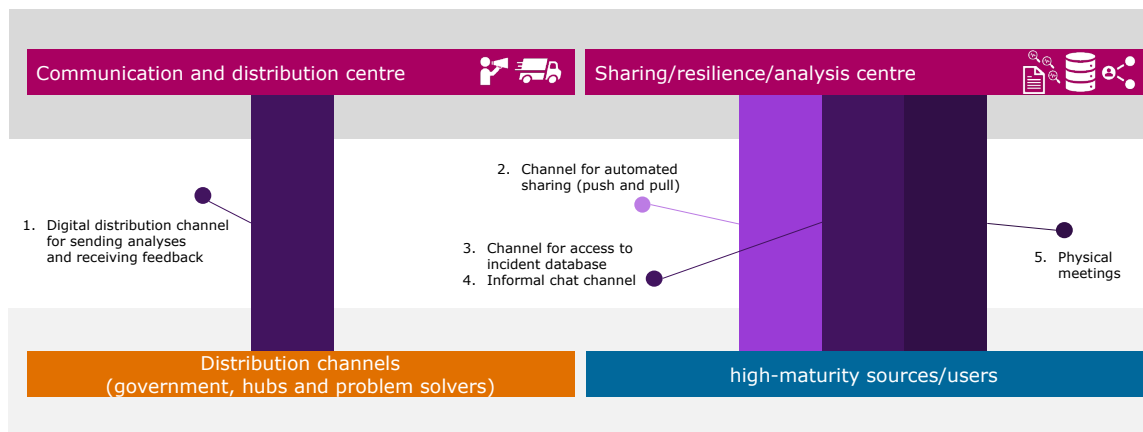


Figure 15 - Channels necessary for the Cyclotron platform

The following channels will be necessary in any event:

1. A digital distribution channel through which analyses are sent and feedback is received. By developing a digital channel, it will be possible to reach new intermediary organisations quickly. The CISP platform in the United Kingdom could be used as an example. It will be important to involve the intermediary organisations in the development of a digital channel so that the format of the information is consistent with the processing method envisaged. The ISPs and MSPs will be particularly important players, because a big group of users can be reached through them.
2. A channel for automated sharing. A channel must be created to which parties can connect with a view to sharing raw data proactively (push) and requesting information (pull). In the short term, it would seem logical to connect to an existing platform that can become operational quickly, such as the Malware Information Sharing Platform (MISP) (which is already used by the NDN).
3. A channel for access to the incident register. It will be important for affiliated parties to be able to gain access to part or all of the incident register, both to provide and request information. A clear framework will need to be developed to determine which party has access to which data and also how the format and quality of data will be monitored. Access may initially need to be limited in line with the 'hit-no hit' principle.
4. An informal chat channel. It will be important to create a channel to promote and support the informal network. In this chat channel, participants will be able to share information with each other about current developments and submit requests to other participants.
5. Physical meetings. To ensure that the informal network is developed and supported properly, it will be important for members of the network to have

regular face-to-face meetings. The same will be essential for the analysis and resilience centre, in which parties will work together to deliver products. Although digital meetings are possible, it would be preferable for parties to work together face-to-face.

Several relevant requirements apply to the channels as well. These are explained in more detail in the table below.

Subject	Requirement
Management and maintenance	Channel management and maintenance must be provided for through the Cyclotron platform.
Security	Obviously, the digital security of the channels must meet current standards.
Compartmentalisation	From a legal point of view, it will be important for data to be stored in such a way that excessively large non-targeted datasets are not created. As such, data compartmentalisation in combination with purpose limitation (see design information) is an important functionality that must be available.
Physical location	To support the informal network, it will also be important to have a permanent, joint, physical location as a home base (campus) of sorts.
Scalability	The channels will need to be sufficiently scalable, so that it is easy to connect new stakeholders.

Table 7 - Requirements for the channels

SPECIAL FRAMEWORK CONDITIONS

The section on the design outlines various framework conditions regarding information, stakeholders and channels that must be met. An in-depth analysis was carried out of a number of these framework conditions during the review, which will be set out in greater detail in this section.

LEGAL FRAMEWORK

The following legislation may be relevant when setting up a public-private partnership platform in which privacy-sensitive information is shared in relation to present or imminent cyber incidents:

- Wiv
- GDPR
- Wbni
- Police Data Act (Wpg)
- Data Processing by Partnerships Act (Wgs) – not yet in force
- Competition Act

A legal framework will be determined depending on the specific choices that are made during the implementation of the Cyclotron platform and the associated framework conditions. A crucial decision at the platform's inception is where it can be subsumed best in legal terms, given the method of information sharing as expressed in the design. Once it has been determined where Cyclotron can be accommodated, an additional review must be carried out regarding the extent to which the intended stakeholders are able to share the desired information on the platform.

Legal accommodation of the Cyclotron platform

The issue of the legal accommodation of the Cyclotron platform starts with identifying the potential data processing operations that are to take place on the platform. *Table 8* shows the various data processing operations that will be involved in any case.

Provision	Centre
1. Provision of data by the organisations involved to other organisations involved: a. Direct provision through the information sharing centre. b. Bilateral provision without the information sharing centre as the intermediary.	Information sharing centre
2. The organisations involved share information relating to incidents with a central incident register and have access allowing (limited) consultation of the register.	Information sharing centre
3. Sharing of specific types of data by the organisations involved with Cyclotron; the collection and further processing (analysis, etc.) of that data within Cyclotron.	Analysis and resilience centre
4. Participation of employees of parties in the joint assessment of the data (analysis) in Cyclotron.	Analysis and resilience centre
5. Provision of data from Cyclotron to distribution channels.	Communication and distribution centre

Table 8 – Data processing operations in the context of Cyclotron

During the review, a survey was carried out with a team of lawyers from the AIVD, the MIVD, the Public Prosecution Service, the NCSC and the National Coordinator for Security and Counterterrorism (NCTV) into the options for the incorporation of the Cyclotron platform into an existing or new organisation. Although a thorough follow-up analysis is required, this survey shows that none of the existing public-sector organisations is a 100% match for the data processing operations provided for in the context of Cyclotron. Particular attention was devoted to the possibility of accommodating the platform with the AIVD (the MIVD was not taken into consideration, as Cyclotron is more likely to operate in the domain of the AIVD than that of the MIVD), the NCSC and/or the police.

With regard to any future legal frameworks, it was explored whether the Wgs could provide an appropriate legal framework for Cyclotron activities. Based on the discussions with the lawyers involved in the development of the Wgs, it was concluded that this new law is insufficiently in line with Cyclotron.

Given that the statutory framework that offers the most options for the aforementioned data processing operations is that of the Wbni, the best match in legal terms is for the platform to be accommodated with the NCSC in the near future.

This means that the following will be possible in the short term:

- Information provision to the platform (NCSC): under their individual legislative frameworks, the AIVD, MIVD, police and Public Prosecution Service will be able to share information with the NCSC in certain cases.
- Data processing on the platform (NCSC): processing of this data must take place with due observance of the Wbni and GDPR.
- Joint assessment on the platform (NCSC): employees of the AIVD, MIVD, police and Public Prosecution Service may be seconded to the NCSC if necessary. Data analysis must take place within the framework of the statutory duties of the NCSC.
- Provision of data from the platform (NCSC): data can be shared with the AIVD and MIVD in various cases. Data sharing with the police and Public Prosecution Service is more restricted under the legislation currently applicable to the NCSC. The NCSC itself primarily shares information directly with central government and critical providers. In addition, the NCSC itself shares information in relation to other providers with the intermediary organisations within the LDS designated under the Wbni. The forthcoming amendment of the Wbni will make it possible for the NCSC to share information in a broader sense with intermediary organisations or with other providers themselves in the absence of an intermediary organisation.





With regard to the long term, there are two realistic options from a legal perspective:

1. Placing Cyclotron under the responsibility of the NCSC based on amended regulations. This entails amending the Wbni to make the duties and primarily the scope with respect to the target group of Cyclotron part of the remit of the NCSC.
2. Establishing Cyclotron in an independent partnership based on new legislation. Although the Wgs initially appeared to be an option for a separate partnership of this kind, it has become clear from discussions with the legal experts involved that this Act is not sufficient for the Cyclotron platform due to the fact that the Wgs is primarily intended for the detection and combating of fraud and serious organised crime. In addition, the processing operations set out in this Act do not fully align with what is envisaged within Cyclotron.

In addition to the legal frameworks, a number of other considerations are equally relevant when choosing the right location for the Cyclotron platform. This is explained in greater detail in the paragraph *Organisational structure and Governance* on page 40.

Table 9 provides a summary of the considerations that played a key role in the conclusions formulated above.

Key:

	No legal match
	Insufficient legal match
	Limited legal flexibility
	Provides sufficient legal flexibility








Organisation	Remit regarding Cyclotron	Considerations	Match
Police (Wpg)	Limited to detection	Purpose and scope of Cyclotron largely exceeds the flexibility provided by the Wpg for the exchange of information.	
AIVD (Wiv)	Limited to national security and other critical interests of the State	In particular, there is scope for the provision of information to the AIVD. Sharing information with third parties is restricted due to the remit of the AIVD.	
NCSC (Wbni)	Limited to primary target group: central government and critical	Due to the fact that the NCSC's target group is limited, joint analysis is limited, and the NCSC can only re-share to a limited extent. A large proportion of the required mature stakeholders already fall within the remit.	
NCSC (new legislation)	Remit fully feasible	The NCSC's remit must be expanded to include several target groups to allow for a wider reach.	
Private foundation	Remit fully feasible	This can be regarded as a so-called U-bend construction due to the major participation of public sector parties. As a result, information provision is therefore not feasible from public parties	
Partnership (based on voluntary agreement)	Remit feasible, but restricted due to GDPR	The combination of various legal frameworks is overly complex and joint analysis does not appear to be feasible.	
Partnership (based on new legislation)	Remit fully feasible	The legislation can be fully adapted to the duties of the partnership.	

Table 9 – Comparison between legal frameworks

The analysis makes clear that **there is no fully appropriate legal framework available in the short term**, which means that the legal framework places

restrictions on the duties of the Cyclotron platform in the beginning. In order to be able to carry out the full package of duties in the longer term, a separate legal framework is envisaged. Due to the fact that the realisation of such a framework will require a lengthy lead time, it is vital that a legal task force gets to work on preparing the new legislation required and initiating the relevant processes immediately following the final decision on the development of the Cyclotron platform. This task force should not restrict itself to this new legislation, but should examine the full legal context and produce workable solutions. Lawyers with knowledge of the legal context of the private stakeholders should be involved.

In particular, the authors of this review recommend that the legal task force examine the following elements:

- Further identify what opportunities there are to share, process and provide information under the Wbni with public and private parties.
- Take into account the effects of the amendment of the Wbni and the NIS2 Directive.
- Carry out an additional review of any potential barriers arising from the GDPR and the Competition Act for private-sector parties in particular.
- Initiate the preparation of new legislation in parallel with the foregoing.

Impact of the GDPR

Following the various discussions with other Dutch initiatives and with a professor of privacy law¹⁰, it has become clear that the GDPR may entail potential barriers to the activities intended within Cyclotron, primarily for private sector parties.

Raw data and analysed information, as shown in Figure 12, may contain personal data. Examples include the IP addresses and email addresses of attackers and victims. The GDPR must be observed when processing personal data.

The public organisations in Cyclotron have a legal basis for the processing and sharing of personal data based on their own legal frameworks. Private sector organisations, however, can only share information on the basis of one of the lawful grounds set out in Article 6 of the GDPR, which inter alia includes the provision that personal data may be processed on the basis of a legitimate interest. The Dutch Data Protection Authority regards ensuring a high level of security and protection of computer systems as an interest that qualifies as a legitimate interest.¹¹ This means that there may be flexibility for private-sector parties to share privacy-sensitive information within the Cyclotron platform.

More difficulties arise if this information must also be analysed. This requires further substantiation of the basis of the legitimate interest. Not all forms of information

¹⁰ The study made use of valuable insights on privacy law from Prof.dr. B.W. Schermer of Leiden University.

¹¹ Dutch Data Protection Authority, guidance on 'legitimate interest' ground –see https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechvaardigd_belang.pdf

exchange within Cyclotron involve the sharing of personal data. When implementing Cyclotron, it would be prudent to develop a number of example situations and analyse them together with specialist privacy lawyers to determine their impact. On that basis, a definitive assessment can take place of whether the information can be processed.

Finally, it is crucial that no large-scale collection of privacy-sensitive data takes place at the information sharing centre. When implementing the design, a technical solution must therefore be chosen that ensures that information is shared directly between the various stakeholders, without (long-term) centralised storage. **A data privacy impact assessment (DPIA) will have to be carried out on this solution prior to implementation.**

Opportunities for scientific research

Based on discussions with representatives from the scientific community, it has become clear that the Cyclotron platform constitutes an intriguing source for scientific research purposes, on the one hand to study what can be learned from a far-reaching form of public-private partnership of this nature, and on the other hand because collected data, such as the incident register, may provide an effective source for scientific research purposes.

Although Cyclotron is not intended as a tool to collect data for the purpose of scientific research, the authors of this review believe it would be prudent not to rule out the possibility of future scientific research in advance. The authors of this review recommend including this element in the development of the future legal framework for Cyclotron, so that the option for further scientific research is kept open.

ORGANISATIONAL STRUCTURE AND GOVERNANCE

In addition to legal concerns, other factors play a key role in the selection of an appropriate and effective organisational structure for the Cyclotron platform. Similarly, the decision in favour of a specific organisational structure depends on a number of choices in the area of governance¹².

Organisational structure

Various factors play a role with regard to the selection of an organisational structure and that of any lead organisation (i.e. an organisation that acts as the owner of the Cyclotron platform). Based on the legal considerations, the authors of this review have arrived at the recommendation to embed the platform within a public organisation.

¹² The review relies on the valuable insights of Prof.dr. E.H. Klijn of Erasmus University Rotterdam in the field of governance in the public-private partnerships.

There are a number of additional considerations in this regard:

1. Building a new organisation versus incorporation into an existing structure. Building a completely new organisational structure requires setting up basic facilities that are already available at existing organisations. If possible, it is preferable to seek alignment with an established organisation, allowing the focus to remain fixed on the substantive development of Cyclotron.
2. Ministerial responsibility. When choosing an organisational structure, it is vital that a decision is made with regard to ministerial responsibility. Choosing an existing organisation as the basis for the Cyclotron platform has the advantage that this is clear in advance. A potential disadvantage may arise if other stakeholders have a different preference with respect to ministerial responsibility, which may negate the choice of an existing lead organisation.
3. Stakeholder involvement. The advantage of a new, separate organisational structure is that the involvement of the various stakeholders can be embedded and safeguarded more easily. If a lead organisation is chosen to act as the owner, the involvement of the other stakeholders in the decision-making process regarding Cyclotron must be organised separately.
4. Connection to and integration with existing initiatives. Cyclotron intersects with various existing information sharing initiatives, including the CIIC, LDS, NDN and SecureNed. There is significant demand for consolidation in the landscape. This is more feasible if the Cyclotron platform were to be embedded in a lead organisation in which the overlap with existing initiatives is highest.
5. Political scope for amendment of existing legislation. In the event the platform is placed under the responsibility of a lead organisation, it will in any case be necessary to expand the existing legislation governing that organisation. When making a decision, it is advisable to take into account the extent to which there is political scope to expand the legislation of the relevant organisation in the context of Cyclotron's remit.

Based on these considerations and following the analysis of the legal framework, the authors of this review have come to the conclusion that **the most prudent decision would be to embed Cyclotron in a lead organisation**. In the estimate of the authors of this review, the development of Cyclotron is a complex operation. There are significant practical advantages to initiating a process of this nature from within an established organisation, thereby automatically establishing ministerial responsibility. With respect to the engagement of the various stakeholders, further safeguards must be embedded into this scenario. This aspect is discussed in the next section.

Subsequently, a decision will have to be made as to what organisation should be the lead organisation for Cyclotron. **The organisation that is most qualified for this role, both in the short and longer term, is the NCSC**. The legal framework of the NCSC already offers flexibility for a start to be made in the near future. An additional legal framework is required for the longer term. With regard to the alignment and

integration with existing initiatives (see the paragraph *Alignment with the existing landscape* on page 46), there is a great deal of overlap with initiatives that are part of the NCSC, such as the LDS, the NDN and SecureNed.

Governance

As stated in the paragraph on organisational structure, the authors of this document have assumed a situation in which a lead organisation would form the basis for the development of the Cyclotron platform. This organisation will have to be prepared to invest manpower and resources into its development. Although the subject of the budget falls beyond the scope of this review, it is recommended that a sufficient budget be reserved for the development of the Cyclotron platform.

The core element of the Cyclotron platform is the public-private partnership. For this partnership to succeed, the various stakeholders must feel a sense of joint responsibility for its development. However, one risk of assigning responsibility for the platform to a lead organisation is that the stakeholders involved may not feel that it 'belongs' to them. When it comes to the governance structure to be chosen, it is therefore vital that the other stakeholders are given room to help shape the decisions on the developments that are taking place.

The following elements are crucial in relation to the decisions on governance:

1. Daily management of the platform. Due to the fact that the platform is to be placed under the responsibility of a lead organisation, there will already be an existing governance structure in place for the management of employees of the platform. This daily management will therefore be provided by the lead organisation. It is essential that the lead organisation should manage its relationships with the various stakeholders and monitor their contribution and engagement.
2. Contractual agreements versus process agreements. It may be necessary to lay down commitments for collaboration with the various stakeholders legally in the form of an agreement or covenant. It is recommended that the agreements should be limited to key points. It is more important that additional process agreements be laid down with the various (groups of) stakeholders, which define the various roles that the different parties can and should play, as well as to establish rules of conduct. In order to obtain and maintain support moving forward, it is vital that these commitments are established in mutual consultation with the stakeholders involved and that it is clear what the common interest is that is being pursued. This will foster more trust and confidence.
3. Strategic engagement through a governance board. In order to ensure that the various (groups of) stakeholders remain closely involved with Cyclotron, it is recommended that a strategic board should be set up to discuss the progress and development of the platform. Within the board, aspects such as evaluations can be discussed, alongside the planning of new developments, as well as examples of successful and less successful initiatives (from which to draw key lessons). Participants will represent a (group of) organisation(s) and will ideally hold a C-

level position within their own organisation. The participants of this board will be drawn from both the public and private domain.

4. Agenda setting consultation. With respect to the analysis and resilience centre, decisions will have to be made in terms of the subjects that are put on the agenda. It is essential that a form of consultation should be introduced at a tactical level in which various experts jointly set the agenda for the coming period. Participants in the consultation will represent an organisation or a group of organisations and will have sufficient subject-specific expertise to be able to weigh up the usefulness and importance of the various topics. A process on the decision-making procedure within this consultative structure must be outlined.

BUILDING A TRUSTED COMMUNITY

One final key aspect to ensure the success of the Cyclotron platform is the answer to the question to what extent a trusted community can be built successfully. The term refers to a group of stakeholders who trust each other to a high degree and are prepared to invest time in the initiative of kickstarting intensive information sharing. The design sets out various framework conditions that directly impact this aspect. These can be classified into the following two categories:

1. Criteria for participation, including the maturity of the participants
2. Building trust

In the following paragraphs, the authors of this document set out a number of considerations for the further development of these framework conditions in relation to the implementation of Cyclotron.

Criteria for participation

The key criterion underpinning being able/permitted to participate as an information provider within Cyclotron is the maturity of the relevant stakeholder. The design refers to three levels of maturity: low, medium and high. There is currently no widely recognised definition of these levels of maturity, and the authors of this review recommend that this should be clarified in more detail in the context of the development of Cyclotron. This requires a diligent approach, and the scope of this review is currently insufficient in this regard, which is why the authors of this report will confine themselves to suggesting a number of avenues of thought.

The NDN already makes use of a number of criteria that were developed in collaboration with TNO, which provide an indication of the maturity of an organisation in the context of connection to the NDN. These criteria can form a point of departure for the further development of a maturity model. More general maturity models that are available on the market, such as CMMI¹³, may likewise serve as input.

Relevant objective elements that emerged from the review in relation to the high level of maturity include:

¹³ <https://cmminstitute.com/cmami>

- The quality of knowledge and experience in dealing with information received about occurring or imminent cyber incidents. Indicators include:
 - Processes in place for handling threat intelligence, such as structural monitoring and CSIRT/CERT activities.
 - Existing infrastructure and use of common standards for the processing of threat intelligence, such as the presence of SOC/SIEM and the application of standards such as STIX (format) and MISP (technical platform).
 - Organised governance in relation to required follow-up actions based on the threat intelligence.
- The ability to analyse incidents autonomously and to report in such a way that this information can be used by other stakeholders.
- The availability of employees with a sufficient level of knowledge and experience to deal with confidential threat intelligence.

Other criteria can also be used in addition to maturity. It has become clear from the discussions that there are concerns about information sharing with private parties that also operate outside the Netherlands or that have an international parent organisation. It may be sufficient to build in safeguards to ensure that information can only be used within the Dutch context (see the paragraph *Building a trusted community* later on in this section). However, this does not provide any guarantees that information will not be shared further. It is also possible to create subgroups for private organisations with a broader operational scope (European, worldwide), such as has been described in the design (see *Building a trusted community*). However, that, too, has its limitations, given that only very limited information will then be shared with the group worldwide and participation for this type of stakeholder may therefore be less opportune. The authors of this review therefore recommend making a clear choice in advance in terms of which scope (the Netherlands, European or worldwide) will be granted to the participants and devoting more attention to additional safeguards, as listed above.

Finally, when determining the final criteria for the participation of private parties, an assessment must take place of whether these criteria have been formulated broadly enough not to cause any market disruption. After all, there is a risk that private organisations may have a (substantial) commercial advantage because they are allowed to participate in Cyclotron compared to organisations that are not permitted to do so.

Building mutual trust

Sensitive information will be shared within Cyclotron. It is therefore necessary that sufficient safeguards are embedded to ensure that participants have sufficient confidence to share any information that they have.

A distinction must be made in this instance between general safeguards and safeguards for specific target groups (see the paragraph *Creating subgroups with specific requirements for shareability* on page 29). These safeguards will have to be

developed for the subgroups as soon as it has been decided to set up specific target groups and the relevant context is clear. This paragraph therefore focuses on general safeguards that can be used to build trust.

The following elements are essential to building trust:

- Establishing agreements and rules of conduct. To ensure a properly functioning community, it is vital that agreements on confidentiality and rules of conduct are established with all stakeholders involved. As set out in the paragraph on governance, it is preferred that these should be developed jointly in consultation with the relevant stakeholders, to ensure that these agreements enjoy a broad base of support.
- Dutch context. A common request is for a safeguard to be embedded that information can only be used within the context of the Netherlands. This requires agreements to be made when entering into a partnership with a private stakeholder on how information may be used, e.g. exclusively to protect Dutch interests. The situation in which information is processed in an organisational unit outside the Netherlands must be taken into account. For example, this can happen if the organisation's Strategic Platform on Cyber Threats (*Strategisch Overleg Cyberdreigingen, SOC*) is located in another country.
- Trust in private stakeholders. With respect to private stakeholders, it is vital to embed additional safeguards aimed at supporting trust and confidence. There are two ways in which these safeguards can be implemented. On the one hand by having the business unit taking part in Cyclotron achieve a certain level of certification. The ABDO 2019¹⁴ (in which security requirements for security contracts of the Ministry of Defence are laid down) may serve as a starting point for the requirements that can be imposed on companies. Alignment could perhaps be sought with the development of the ABRO (a comparable instrument that is being developed for central government as a whole). A second element that can be used is a screening process for the relevant employees of the organisations taking part.
- Informal network. The informal network is of vital importance in relation to building trust between stakeholders. The better the parties involved in information sharing know one another, the better the flow of information will get going. It is therefore crucial that sufficient attention is devoted to building this network at all levels involved: operational, tactical and strategic level. The strategic level is of particular importance. By organising engagement and enthusiasm at a strategic level, the right support is created to make employees available for Cyclotron activities at an operational level. It is recommended that sufficient attention be devoted to this issue.

¹⁴ <https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/downloads/beleidsnota-s/2020/02/04/abdo-2019>

ALIGNMENT WITH THE EXISTING LANDSCAPE

FUTURE VISION: INTEGRATION OF EXISTING INITIATIVES

The analysis of the current landscape in the area of information sharing within the cyber domain (see the section on the current landscape for information sharing on page 9 and onwards) shows that there are many valuable initiatives that partly complement one another, but also partly overlap. A number of these initiatives come together in the Cyclotron platform and are supplemented with additional activities.

In order to implement the Cyclotron platform successfully, it is critical that these initiatives are effectively linked up with the existing landscape and to make improvements where possible. For example, there is a need for more centralised management in the information sharing landscape, both for public and private parties (see Table 1). In addition, a critical success factor has been defined that is related to the current landscape (see the paragraph *General shortcomings and needs* on page 15), viz. that it is vital to consolidate the landscape and link any new initiative to the existing initiatives in order to prevent more fragmentation.

The design of the Cyclotron platform shares the most common ground with the following initiatives (see *Modelling of initiatives in the information sharing landscape* on page 58 for details on these initiatives):

- CIIC
- LDS
- NDN
- SecureNed

Due to the many ways in which the various initiatives and the platform intersect, the authors of the review have identified the following opportunities for consolidation in the landscape:

1. Building Cyclotron as part of an already existing initiative and thereby avoiding the addition of another initiative to the landscape.
2. Merging a number of the existing initiatives with Cyclotron gradually over time to ensure a greater degree of cohesion and efficient use of manpower and funds.

The paragraphs below outline how the four aforementioned initiatives relate to the design of the Cyclotron platform in greater detail and how a partnership or integration can take shape in future.

RELATIONSHIP WITH THE CIIC

The CIIC intersects with the Cyclotron platform in two key areas (see *Figure 16*):

1. Information sharing centre
2. Analysis and resilience centre

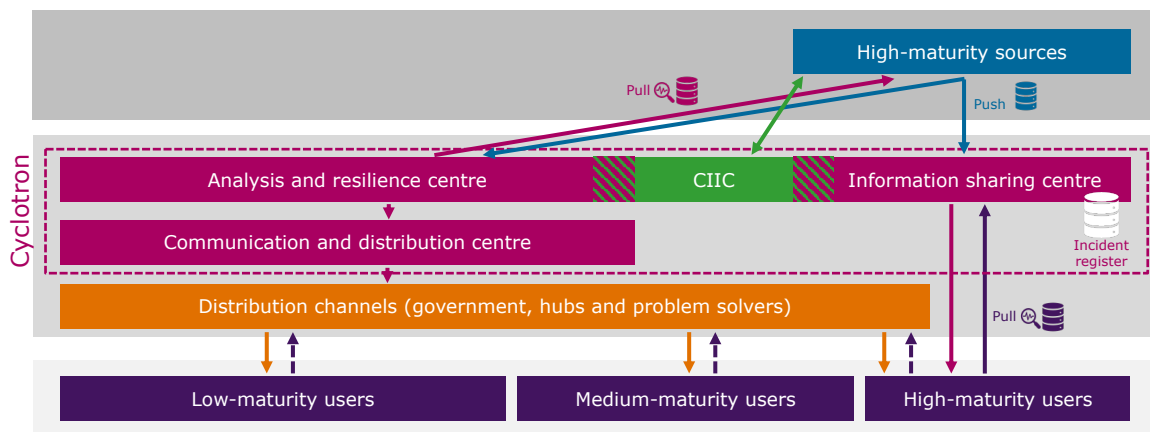


Figure 16 – Relationship between Cyclotron and the CIIC

Although the CIIC maintains its own bilateral relationships with various highly mature stakeholders, it would be beneficial for the CIIC to connect to the raw data that is shared through the information sharing centre. In some cases, the CIIC itself has also identified an opportunity to share information (push) and there may equally be a need to request information (pull). However, highly confidential (classified) information will almost always be involved, which means that cooperation can only take place with a limited group of accredited stakeholders. This aligns with the design principle of subgroups as detailed in the paragraph *Creating subgroups with specific requirements for shareability* on page 29. It is recommended that the CIIC be involved in the development of a subgroup for the sharing of highly confidential (classified) information.

The CIIC could also participate in the analysis and resilience centre, in which case the partnership would mainly focus on analysis and advice. Restrictions would also apply in this case if highly confidential (classified) information were included in a particular analysis. However, it is equally possible for the CIIC to use information for an analysis

or action framework which is not classified, but which is relevant to the development of the product in question.

Looking at the remit of the CIIC, some tasks do not overlap any further with the Cyclotron platform, but are and shall remain relevant. Looking to the future, the authors of this document see the Cyclotron platform and the CIIC as two separate entities that coexist, but maintain a close partnership in the areas outlined above (information sharing centre and analysis and resilience centre).

RELATIONSHIP WITH THE LDS

The focus of the LDS in particular is on ensuring that the widest possible group of clients is reached through various distribution channels. This means that overlap is greatest with the communication and distribution centre (see Figure 17). The NDN connection that is also established through the LDS is not considered here (see the next section).

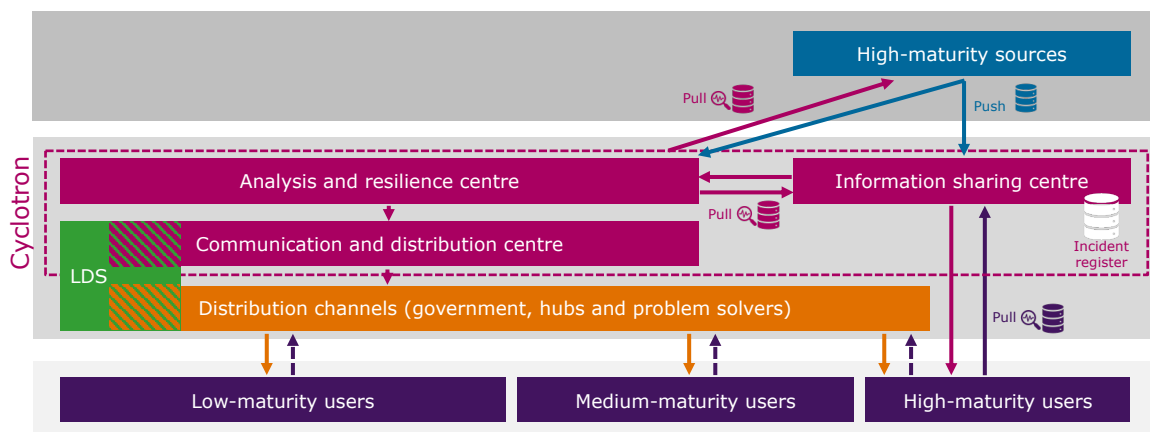


Figure 17 – Relationship between Cyclotron and the LDS

In the future, it will be possible to integrate the activities of the LDS with those of Cyclotron in order to achieve national coverage from a single coordination point. The authors of this review recommend that this be taken into account in the future development of the LDS.

RELATIONSHIP WITH THE NDN

Among other things, the remit of the NDN includes sharing technical characteristics of threats, which overlaps with the remit of the information sharing centre. The overlap primarily centers around the MISP channel that is used for information exchange with critical organisations, CERTs and OKTT organisations. The overlap is illustrated in Figure 18.

Within the NDN, a more limited set of information is shared than is desirable within Cyclotron in the future. Another key difference with Cyclotron concerns the stakeholders. This is a more limited group than envisaged by Cyclotron moving forward (this more limited group is a result of the NCSC's current remit).

Finally, the aim is for the exchange of information within Cyclotron to go in two directions. Although this is technically possible within the NDN, this option is rarely used in practice.

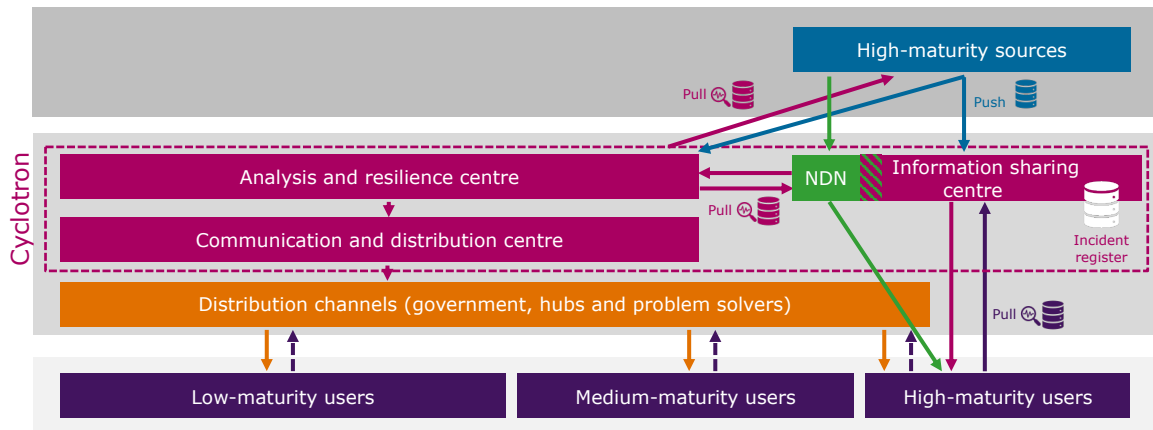


Figure 18 – Relationship between Cyclotron and the NDN

The NDN has a properly functioning mature infrastructure of channels that aligns with what is needed within Cyclotron. The MISP channel, for example, is now widely accepted among the 80+ stakeholders within the NDN.

This means that there are good opportunities available for integration. It also means that the NDN could be selected to serve as a starting point from which to build the Cyclotron platform. Based on a number of additional considerations, the authors of this review conclude that this applies to SecureNed to an even greater degree. It is therefore recommended that the integration of part of the NDN (related to MISP) with Cyclotron be examined and enabled moving forward.

RELATIONSHIP WITH SECURENED

SecureNed overlaps with the Cyclotron design in several regards:

1. Information sharing centre
2. Incident register
3. Analysis and resilience centre

RECOMMENDATIONS FOR NEXT STEPS

The previous sections sought to develop and detail the design of the Cyclotron platform and corresponding framework conditions as much as possible. If the actual implementation of such a platform is decided in the SOC, it is advised that the following recommendations be adopted.

USE THE CYCLOTRON DESIGN AS A BLUEPRINT

Based on broad input from stakeholders in the public domain, private domain and scientific community, a design has been drawn up for the Cyclotron platform (see the sections *Design of the cyclotron platform* on page 23 and *Special framework conditions* on page 35). This design has a very broad scope and cannot be realised in its entirety in the short term for several reasons.

The authors of this report therefore recommend that this design be used as a blueprint for the future. In the short term, this blueprint can be used to make decisions based on legal and practical considerations for the components that can already be developed at this stage.

EMBED THE PLATFORM WITHIN THE NCSC

As set out in the paragraphs *Legal framework* and *Organisational structure and Governance*, the authors of this report recommend selecting a lead organisation that is responsible for the development and implementation of the Cyclotron platform. There are practical advantages to starting such a complex development process from within an established organisation.

As far as the legal framework is concerned, the authors conclude that the NCSC offers the best opportunities for that purpose, both in the short and long term. With regard to the alignment and integration with existing initiatives (see the paragraph *Alignment with the existing landscape* on page 46), there is a great deal of overlap

with initiatives that are part of the NCSC, such as the LDS, the NDN and SecureNed. Moreover, the NCSC is already regarded as a central hub in the field of cyber resilience in the Netherlands by the national and international landscape.

The authors of the review therefore recommend that the Cyclotron platform be embedded within the NCSC.

START DEVELOPMENT OF THE LONG-TERM LEGAL FRAMEWORK IMMEDIATELY

Not all of the intended activities of the Cyclotron platform can be carried out at present due to limitations within the legal frameworks currently available. As outlined in the paragraph *Legal framework*, it will be necessary to develop additional or new legislation in order to enable the full range of activities.

Due to the lengthy lead time required for legislative processes, the authors of this review strongly advise that a legal team be put together immediately at the start of implementation to define the various processing operations in greater detail and develop an appropriate legal framework. In the short term, this legal team can determine what information may be shared at this stage, and it can make a start on developing new legislation for the long term.

This legal task force should not restrict itself to new legislation but should also examine the full legal context in more detail and come up with workable solutions. For example, it is recommended that this task force also involve lawyers with knowledge of the legal context of the private sector stakeholders.

ESTABLISH A GOVERNANCE BOARD AND AN AGENDA BOARD

The effective collaboration and commitment of the stakeholders is essential to ensuring the success of the Cyclotron platform. Because the initiative lies with a lead organisation, this collaboration must be properly embedded and safeguarded in the governance structure (see the paragraph *Organisational structure and Governance*).

In addition to jointly coming to and laying down agreements on collaboration, the authors of this exploratory research wish to emphasise that it is vital that a strategic governance board be set up from the start, consisting of representatives of stakeholders and stakeholder groups (preferably at C level). Once the analysis and resilience centre has been developed, an agenda board will have to be set up that consists of subject-specific specialists who have in-depth knowledge of developments in the field and are jointly able to determine an effective agenda.

MAKE A QUICK START BY LINKING TO SECURENED

The analysis and design revealed that it would be unwise to set up an additional initiative alongside the existing initiatives. The authors of this review therefore recommend consolidating the landscape (integration of existing initiatives over time)

and linking the development to one of the existing initiatives. The highest degree of overlap is with (part of) the NDN and with SecureNed.

Although both initiatives are good candidates as a starting point, the authors of the report recommend connecting the Cyclotron platform to SecureNed. The NDN is particularly strong in the area of information sharing and already has a mature infrastructure in place that can be used for that purpose (MISP). Those elements should be integrated and expanded within Cyclotron. Key new elements in the design include joint analysis (pull mechanism) and the development of an incident register. SecureNed has already gained practical experience with regard to these elements and the unique framework conditions, such as anonymisation, involved.

Finally, SecureNed uses an Agile methodology¹⁵ for the development of new elements for this platform. In the opinion of the authors of this review, this is an approach that may align effectively with the development of the Cyclotron platform. The methodology involves concrete results being achieved step by step, which can further bolster confidence in the initiative.

Instead of developing a very large project like Cyclotron using major goals, a high degree of complexity and a lengthy lead time, linking up with SecureNed will ensure that the first results can be realised in the short term and that the development of the platform can keep up with current events and developments.

The name SecureNed could serve as the name of the Cyclotron platform to reinforce the point that no additional platform will be added to the landscape. If the name SecureNed is insufficiently suitable, it could be replaced by a new name that can count on broader support. It is vital that any new name should have a recognisable narrative and a strong brand value.

DESIGN A SEPARATE SOLUTION FOR TARGET AND VICTIM NOTIFICATION

The review revealed that there is a need within the landscape for an effective solution with respect to target and victim notification.

Target notification relates to informing (individuals and) organisations that they have vulnerable infrastructure that may be a potential target for cyber attacks. These vulnerabilities may have come to light as a result of investigators' efforts (i.e. the volunteers at DIVD may be actively scanning for vulnerabilities) although they may equally be discovered by accident during work carried out by security companies. Victim notification revolves around informing individuals and organisations of which it is clear that they are victims of a cyber attack, but who may not be aware of this yet.

¹⁵ Agile is a methodology that focuses on agility. It was originally developed for software in 2001, but is now used more widely in the development of products and services.

This information may, for example, come to light in the event that an investigation discovers a Command and Control server that contains the data of targets of cyber criminals who are working on (preparing for) a ransomware attack on these targets.

The discussions with the authors of this report made clear that the need for a solution of this kind is widely felt, both within the public and private domain, and that in practice there is no public sector organisation that manages and carries out this remit from a natural position. Fragmented notification activities do take place based on independent remits – for example, those aimed at specific target groups (target notification by the NCSC with respect to critical organisations and by the DTC with respect to non-critical businesses). Certain organisations possess the information, but are insufficiently flexible in terms of both their remit and capacity (such as the police). Moreover, it is currently illegal for the government to seek out target information (scanning) actively.

An initiative that focuses on target notification has recently been launched in the private sector in the form of the Dutch Security Hotline (Nederlands Security Meldpunt). A discussion with representatives of this centre revealed that this initiative was set up due to the fact that target notification has not (yet) been addressed by the government at a central level and there was a sense of urgency to rapidly follow up these types of discoveries.

Although target and victim notification strictly speaking also involves information exchange, it is less suited to the design of the Cyclotron platform. The design primarily focuses on informing one another rapidly regarding threat intelligence (information sharing centre) and jointly analysing and sharing this type of information (analysis and resilience centre, communication and distribution centre). The development of these centres is an extremely complex endeavour. The authors of this report fear that the important issue of target and victim notification will not be afforded a sufficient degree of attention and prioritisation as a result.

They therefore recommend that a separate solution be developed with the relevant private and public partners for this issue, which has a very clear scope. It is vital in this regard that the public stakeholders involved consider to which degree this is a government responsibility and what is required to implement it.

ANNEXES

INFORMATION MODEL

Various types of information are shared within the information sharing landscape. As outlined in the paragraph *The Dutch landscape for sharing information about cyber incidents*, a model has been created within Cyclotron of the types of information that can be shared. This overview helps maintain a clear and unambiguous language with respect to the information to be shared and provides insight into the enormous scope of the subject.

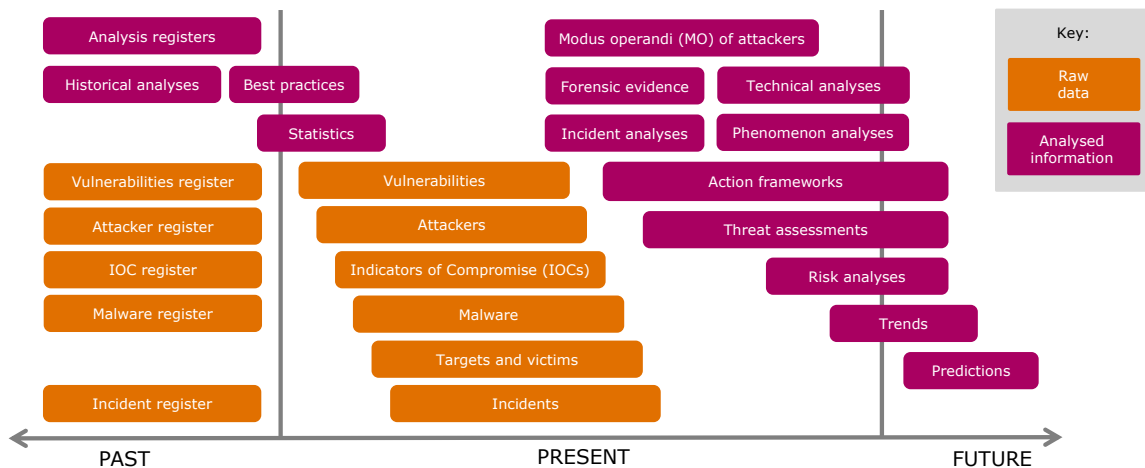


Figure 20 – Information model

Figure 6 has been repeated above and a brief description of each element in the model is provided in this annex. Where possible, the definition of the Cybersecurity Dictionary (*Cybersecurity Woordenboek*)¹⁶ has been followed. These words are marked with an *.

¹⁶ <https://www.cybersecuritywoordenboek.nl/>

Raw data	Description
Attackers*	A party who deliberately attempts to disable or bypass security in order to gain access to a digital system.
Targets and victims	Targets refer to either persons or organisations that can become victims of a cyber attack, for example, because they use vulnerable systems or because they have been targeted by an attacker. Victims may refer to persons or organisations that have been affected by a cyber incident.
Incidents*	An event or activity in which the security of the hardware, software, information, process or organisation may have been compromised or has been compromised either wholly or in part.
Indicators of Compromise*	Information that can be used to ascertain whether a particular party has carried out an attack on one of your assets. The information will often contain characteristics of an attacker, of an attack method or of the malware. For example, if intelligence has revealed that a specific attacker carries out attacks from a particular IP address, that IP address can be used as an indicator of compromise. If there are traces of connections with the IP address on your own digital system, it is clear that the attacker may have attempted to attack you.
Vulnerabilities*	Flaws in digital systems that allow an attacker to gain access to the systems. The attacker can then access information or applications in the system when he or she is not authorised to do so. Or the attacker can ensure that the user is no longer able to access this information or use the application.
Malware*	Malicious software that attackers place onto a digital system in order to be able to access or destroy the system or steal information remotely. Malware is a contraction of the English term malicious software.
Registers	Collections of (historical) data.

Information analysed	Description
Best practices*	A type of technology, working method or activity that has proven to be effective in practice.
Threat assessment	An assessment of something (an event) that may threaten or cause damage to an organisation, such as a malfunction, reputational damage or financial loss (its consequences).

Phenomenon analysis	These are analyses that study a broader phenomenon, such as an analysis that focuses on how ransomware groups operate or how wiper malware is used by state actors.
Forensic evidence	In this context, the term relates to digital forensic evidence. These are professionally recorded traces from a digital investigation.
Action frameworks	Tools aimed at providing advice on how to act in a specific situation.
Historical analysis	An analysis of historical data for the purpose of understanding specific events that occurred in the past.
Incident analysis	An analysis of a cyber incident.
Attacker MO	A unique modus operandi or method used by an attacker or group of attackers to carry out cyber attacks.
Registers	Collections of (historical) data.
Risk assessment*	A method used to gain insight into potential risks. Among other things, the assessor will look at the following: What is the probability of an incident taking place? What would be the impact of that incident?
Statistics	Quantitative data resulting from examining trends, patterns and relationships using quantitative data.
Technical analysis	Analysis of the technical circumstances of a specific event.
Trends	Long-term development in a particular direction.
Prediction	A statement about the things that can be expected on a specific issue.

MODELLING OF INITIATIVES IN THE INFORMATION SHARING LANDSCAPE

This annex provides a visual representation of the initiatives explored according to the modelling in terms of information, stakeholders, and channels.

Cyber Intel/Info Cel

In the context of the implementation of the National Cybersecurity Agenda 2018, the Cyber Intel/Info Cel was set up in 2020¹⁷, in which the AIVD, MIVD, police, NCSC and Public Prosecution Service aggregate relevant intelligence on cyber threats and incidents. Employees of these parties work together in person at the CIIC and assess the information on cyber threats and subsequently pass that information on to one or more of the participating parties for further use if they consider this necessary in connection with the performance of these parties' duties.

Information

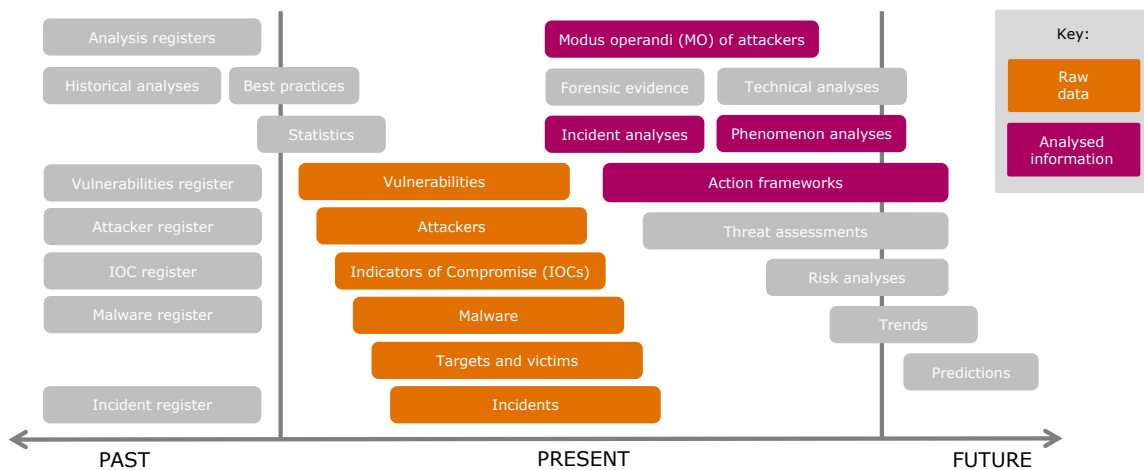


Figure 21 – CIIC information

The information that is exchanged within the CIIC is mainly operational, and is generally shared with the relevant stakeholders under TLP.AMBER and TLP.RED. Phenomenon analyses were not performed at the time of the interview, but are scheduled to be added in the near future.

¹⁷ <https://zoek.officielebekendmakingen.nl/stcrt-2020-30702.html>

Stakeholders

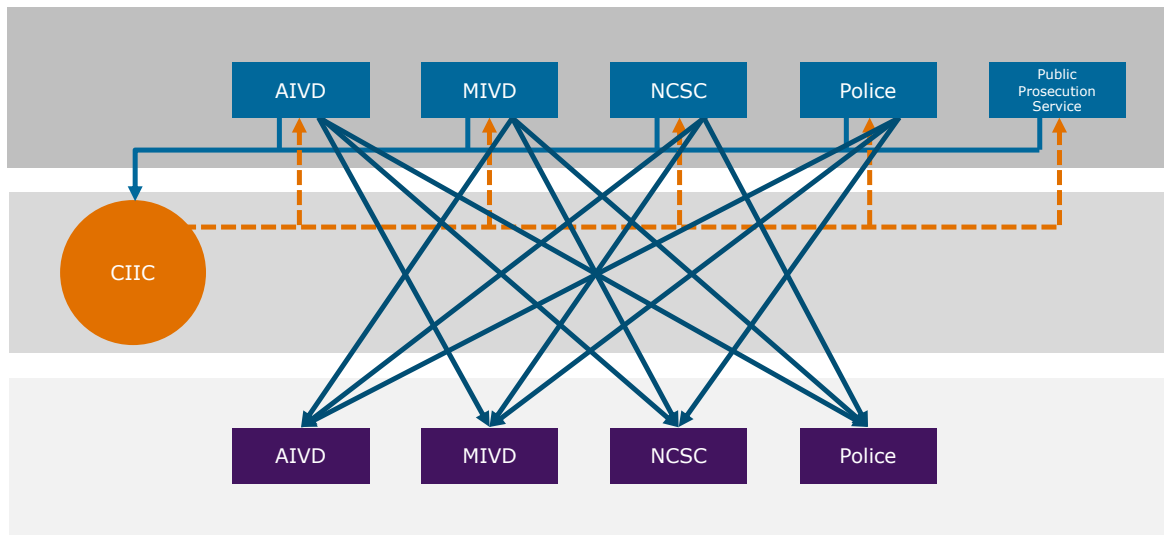


Figure 22 – CIIC stakeholders

Stakeholder roles:

- All CIIC participants are both sources and clients

Information flows:

- Information from 1 or more organisations are brought together in the CIIC for a situational assessment guided by the Wiv as the legal framework
- Information shared within the CIIC remains within the CIIC
- Follow-up actions are followed up by the client under its own legal framework

Channels

Channel	Description
Partner systems	Each partner has its own seconded employees within the CIIC who can consult the source organisation's own channels. The output likewise goes through the existing channels of the specific stakeholder providing the output. There are channels at different levels of classification.

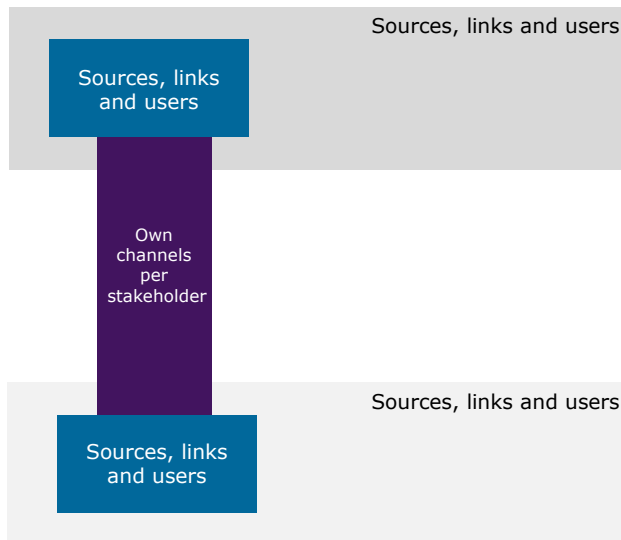


Figure 23 – CIIC channels

LDS

In the LDS¹⁸ the NCSC and DTC collaborate with public and private organisations to exchange information and knowledge. Organisations within the LDS are designated as CERTs or as OKTTs by the NCTV and the NCSC in order to enable the mutual exchange of information within the confines of the law. A CERT or OKTT is an intermediary organisation that represents a larger group of organisations and can also pass on information received from the NCSC to the rank and file.

Information

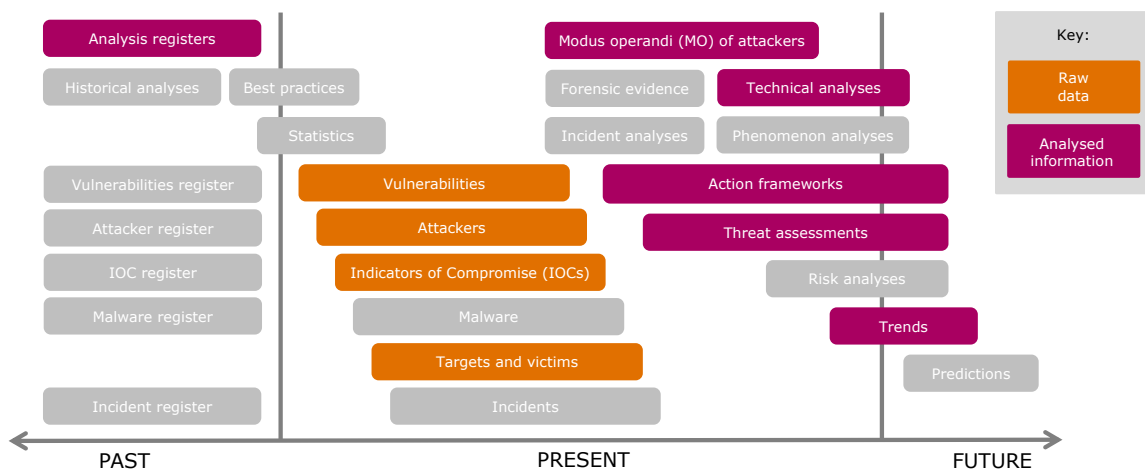


Figure 24 – LDS information

The information exchanged within the LDS is operational and tactical. It is shared among TLP.WHITE, TLP.GREEN and TLP.AMBER. The technical analyses are shared to a limited degree and only after mutual agreement.

¹⁸ <https://www.ncsc.nl/onderwerpen/samenwerkingspartner-worden/aansluiting-op-het-landelijk-dekkend-stelsel-lds>

Stakeholders

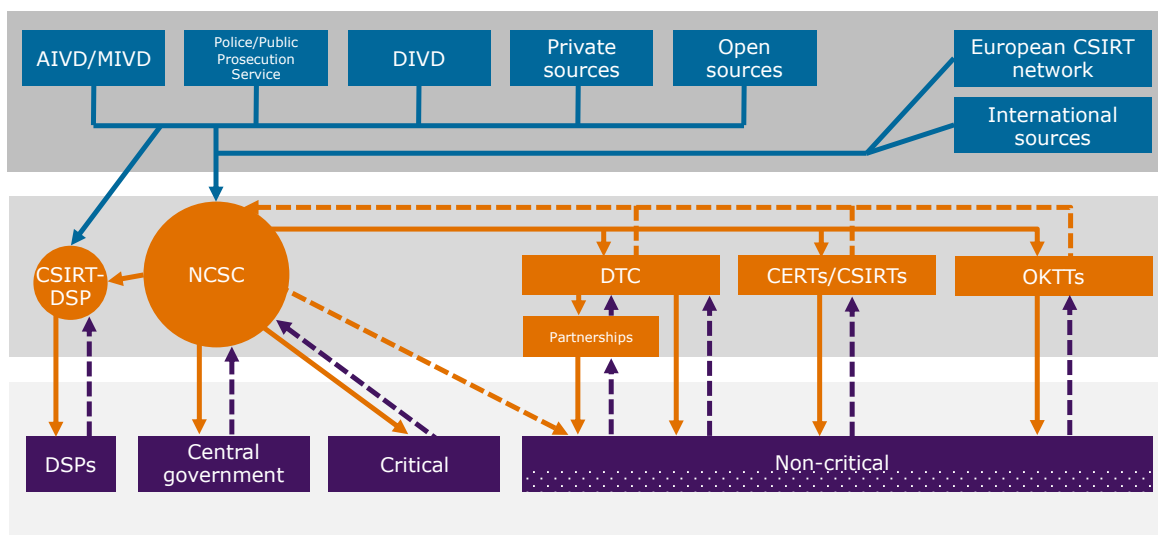


Figure 25 – LDS stakeholders

Stakeholder roles:

- Within the LDS, the NCSC operates as a hub in the network in relation to other intermediaries
- The degree of maturity of the intermediaries varies

Information flows:

- The system does not yet have full nationwide coverage and non-critical organisations are only partially reached
- Information occasionally flows back from clients to links and to the NCSC, but not structurally

Channels

Channel	Description
MISP	An open source solution for information sharing
Tip	A commercial solution (from EclecticIQ) for information sharing
Sensors	Sensors for monitoring based on indicators of compromise
Mattermost	A chat platform for exchanging urgent information
Signal	A chat platform to rapidly contact C-level Cyberveilig Nederland members
Email	This (PGP encrypted) channel is used for sharing vulnerabilities, targets and victims (also known as abuse info) and threat analyses
Website	For the public and broad sharing of advisories

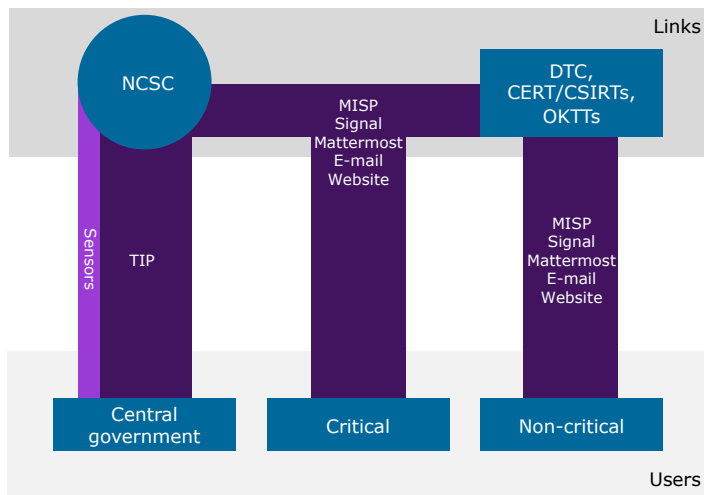


Figure 26 – LDS channels

NDN

The NCSC, the AIVD and the MIVD gather information about cyber threats and make this information available to the NDN.¹⁹ Within the NDN, the NCSC uses the information to draw up a broad and joint assessment of current cyber threats. Organisations that take part in the NDN are also able to furnish information themselves. NDN participants are provided with a platform and sessions are held at which participants can meet face-to-face. Participants share best practices with one another and are able to work on analysing current threats and attacks in a trusted environment.

Information

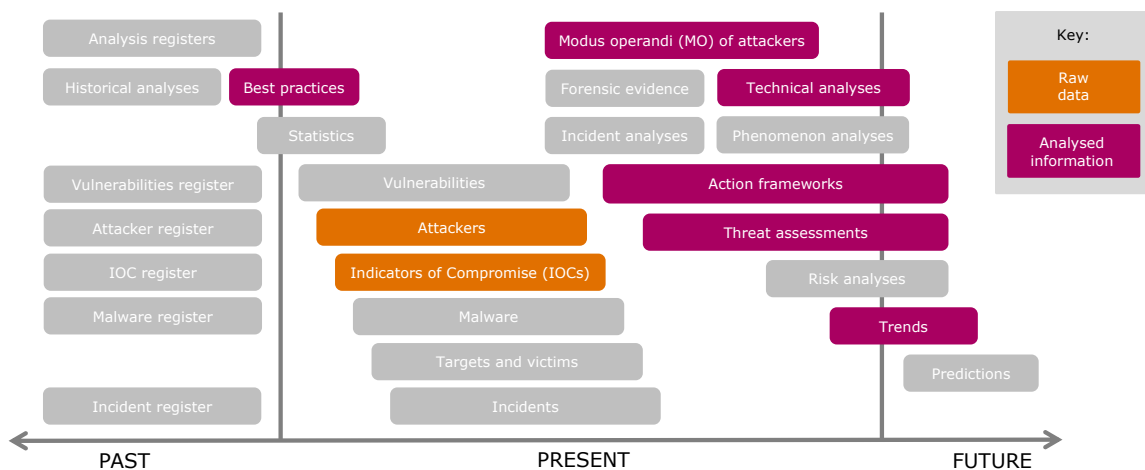


Figure 27 – NDN information

¹⁹ <https://www.ncsc.nl/onderwerpen/nationaal-detectie-netwerk-ndn>

The information that is exchanged within the NDN is operational and tactical, and it is shared under TLP.GREEN, TLP.AMBER and TLP.RED. The technical analyses are shared within a limited community and only with mutual agreement.

Stakeholders

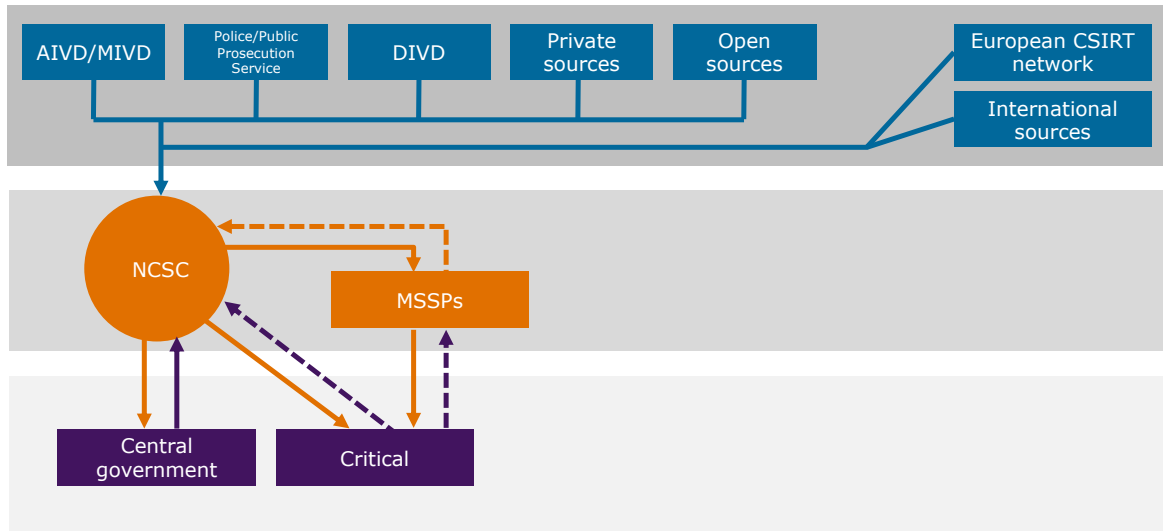


Figure 28 – NDN stakeholders

Stakeholder roles:

- The NCSC is both a source and an intermediary
- Managed Security Service Providers (MSSPs) that are providers to a critical organisation are able to join the NDN on behalf of this client

Information flows:

- Information does not flow back to the NCSC systematically
- Sensors for detection are embedded within central government
- The NDN reaches several links and clients through the LDS

Channels

Channel	Description
MISP	An open source solution for information sharing
Tip	A commercial solution (from EclecticIQ) for information sharing
Sensors	This solution also involves sensors being placed within the network of central government for monitoring based on indicators of compromise
Mattermost	A chat platform for exchanging urgent information
Email	This (PGP encrypted) channel is used to share threat analyses

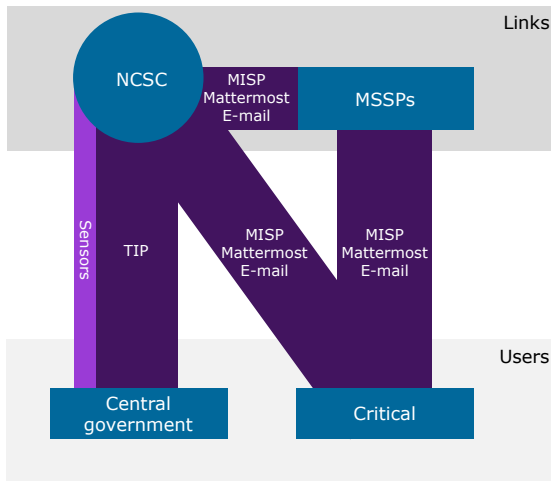


Figure 29 – NDN channels

SecureNed

Government agencies and Dutch companies that collect information relating to cybersecurity through monitoring, detection and/or incident response are able to participate in SecureNed²⁰. In SecureNed, participants report digital attacks or complete brief surveys. SecureNed provides a trusted and safe environment for participants to share information with one another. Based on that information, the NCSC creates a broad and shared assessment of current cyber threats and incidents in the Netherlands. The NCSC frequently informs participants by way of aggregated results of reports and surveys, enriched with the insights of the NCSC. Within SecureNed, information can be shared both openly and anonymously.

This is an initiative that is still in development.

Information

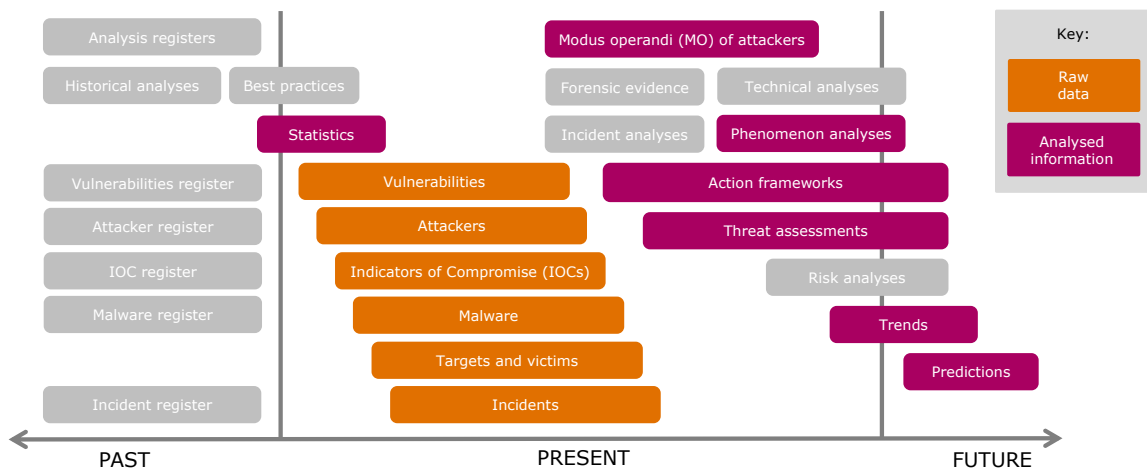


Figure 30 – SecureNed information

²⁰ <https://www.ncsc.nl/onderwerpen/secureded>

Information within SecureNed is mainly operational and tactical. Sharing takes place under TLP.GREEN and TLP.AMBER.

Stakeholders

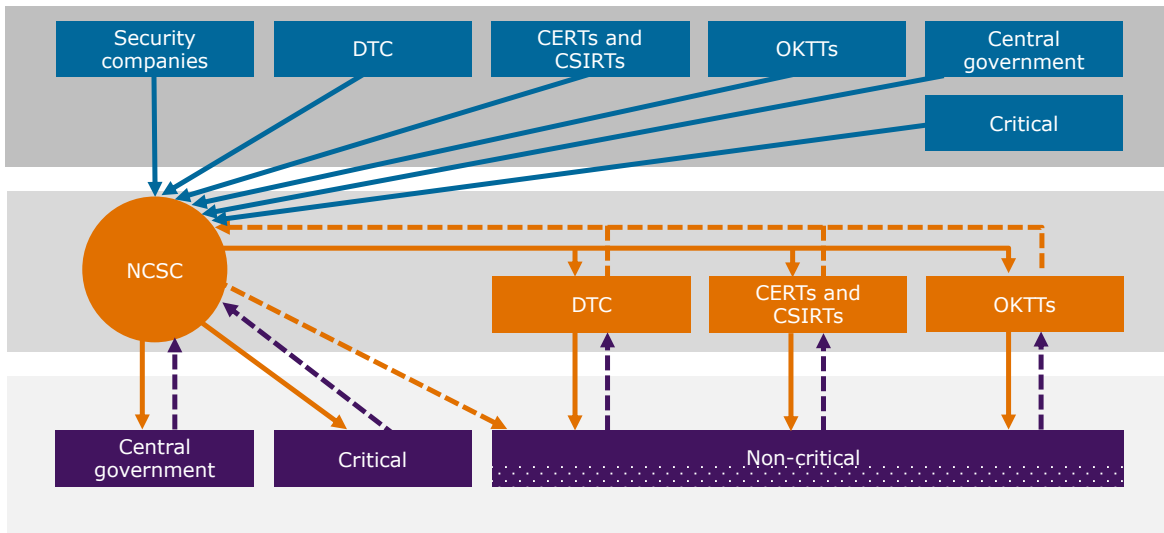


Figure 31 – SecureNed stakeholders

Stakeholder roles:

- CERTs/CSIRTs and OKTTs have an intermediary role vis-à-vis members with regard to requesting and receiving information

Information flows:

- The information is survey-driven
- At a later stage it will be possible to proactively report to SecureNed (Q1 2022)
- The output is only distributed to the parties that have also provided input

Channels

Channel	Description
SecureNed	A web application based on multi-party computation that is used to anonymously retrieve responses to surveys. At present it is reactive, however, from Q1 2022 it will become proactive (by feeding information to the channel in an unsolicited fashion). In time, the channel will offer the possibility of machine-to-machine exchange.

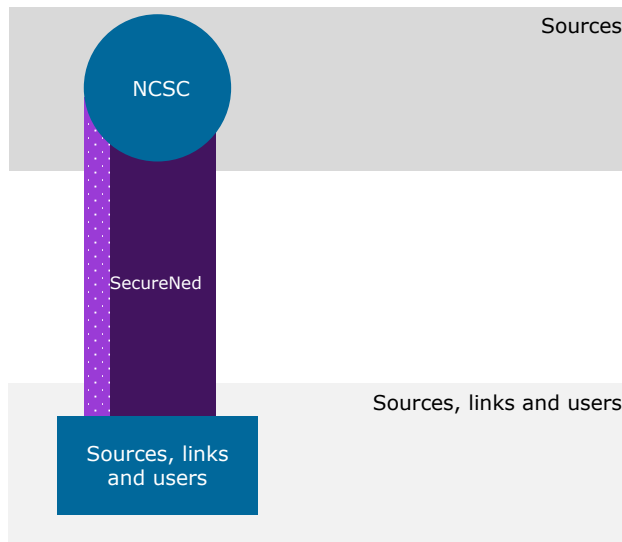


Figure 32 – SecureNed channels

Information Sharing and Analysis Centres

Various Information Sharing and Analysis Centres²¹ (ISACs) operate within the Netherlands. Within this form of consultation on cybersecurity, organisations from the same sector exchange sensitive and confidential information about incidents, threats, vulnerabilities and measures. This primarily takes place in (closed) sessions.

Within any ISAC, participants also have a network of ICT and cybersecurity specialists. By working together with other organisations, which, in turn, have different knowledge of and experience with digital attacks, they are able to join forces in relation to incidents that affect the sector.

Information

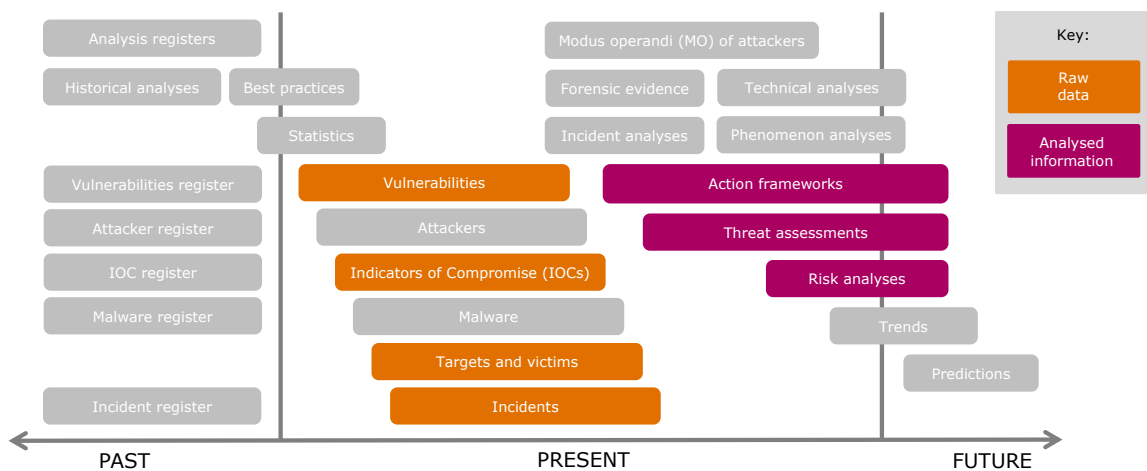


Figure 33 – ISACs information

²¹ <https://www.ncsc.nl/onderwerpen/start-een-samenwerking/zelf-een-samenwerking-starten/samenwerking-sector>

Within the ISACs, operational and tactical information is shared, and this takes place under TLP.GREEN, TLP.AMBER and TLP.RED. Threat assessments and risk assessments are only shared in ISACs with a higher level of maturity.

Stakeholders

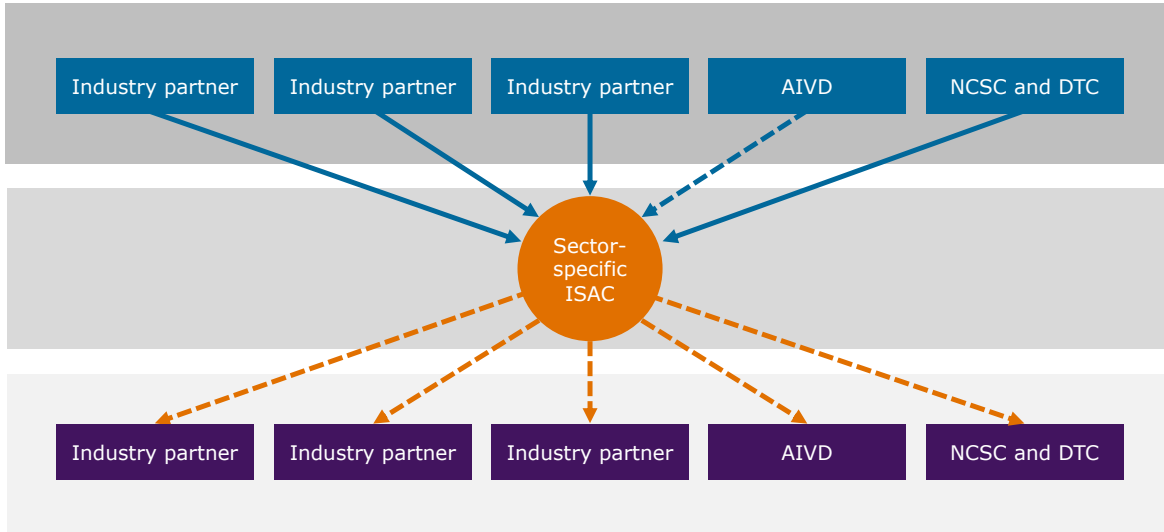


Figure 34 – ISAC stakeholders

Stakeholder roles:

- The exchange effectively takes place within the ISAC
- The NCSC and the DTC provide the ISACs with input and support, such as providing communication channels

Information flows:

- The information is aggregated in the ISAC from and to participants
- Information is also shared on a cross-sector basis, partly through the NCSC, for example, through semi-annual consultations, or between parties

Channels

Channel	Description
Consultation	Most exchange of information takes place through face-to-face forms of consultation
Email	Information that has to reach clients rapidly is shared through (secure) email
DTC platform	The DTC has set up a digital platform in which members of an ISAC can share information with one another in a protected environment. A number of ISACs make use of this facility

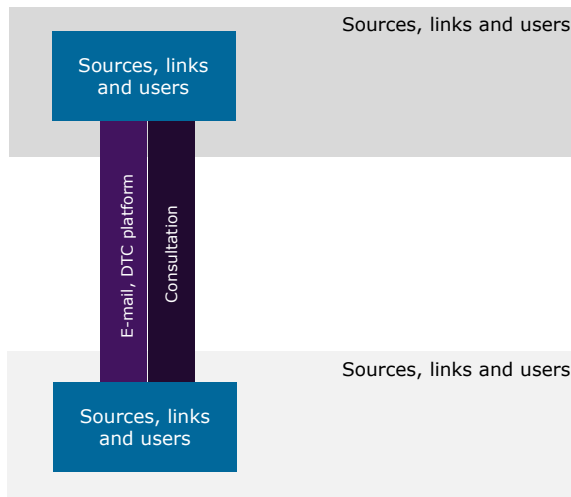


Figure 35 – ISAC channels

Dutch Security Hotline

The Dutch Security Hotline for Cybersecurity (Nederlands Security Meldpunt voor Cybersecurity) is an operational distribution centre for receiving and sharing actual occurrences of abuse (information about undesirable configurations, vulnerabilities and unauthorised use) with all organisations that do not directly receive information through the NCSC.

The Dutch Security Hotline is a private sector initiative that was realised by six foundations: AbuseIO, AmsIX, Connect2Trust, DIVD, NBIP and SurfCERT.

At the time this exploratory research was conducted, this initiative was not yet operational. The analysis is limited to the information and stakeholders and is based on the plans presented.

Information

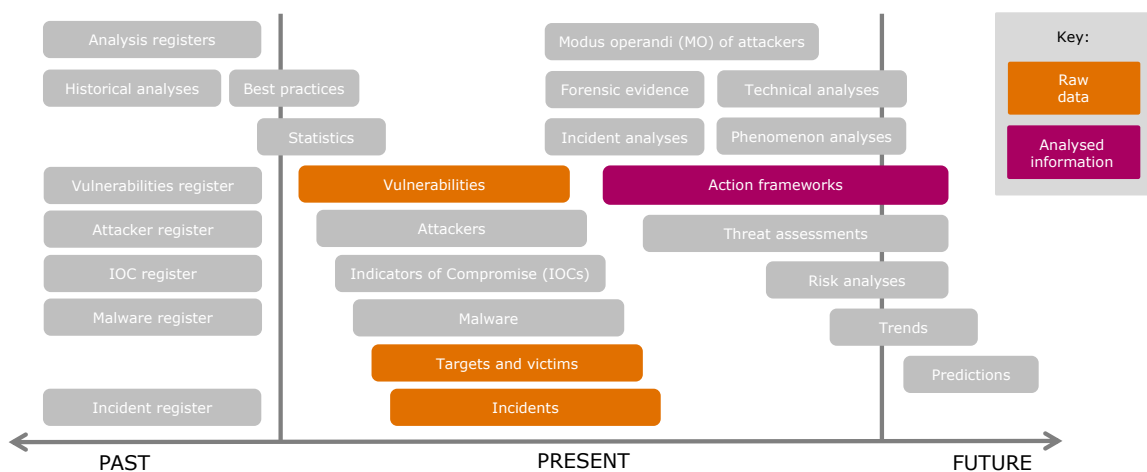


Figure 36 – Dutch Security Hotline information

For the time being, only operational information is shared within the Dutch Security Hotline. Additional information was not yet available at the time this research was conducted.

Stakeholders

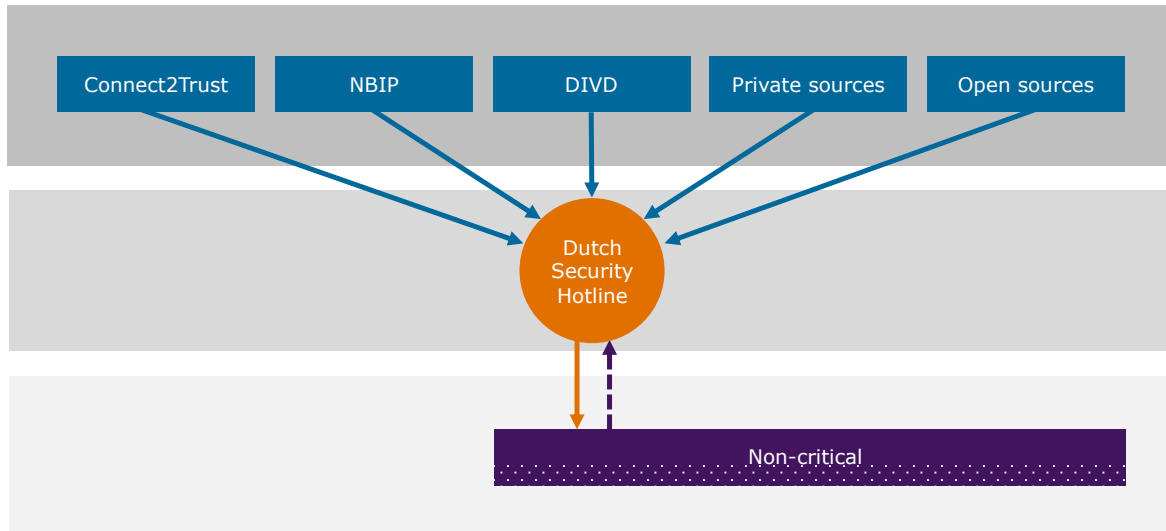


Figure 37 – Dutch Security Hotline stakeholders

Stakeholder roles:

- The initiators are Connect2Trust, NBIP and the DIVD
- Connect2Trust and NBIP are part of the LDS as OKTTs

Information flows:

- The starting point for the initiative is that clients are notified in an unsolicited fashion
- The aim is to reach non-critical businesses as much as possible, but it is unclear whether this is feasible

OVERVIEW OF FOREIGN INITIATIVES

Canada – CCCS

Canada's national CSIRT is the Canadian Centre for Cyber Security (CCCS²²) and is part of the Canadian intelligence service, the Communications Security Establishment (CSE). The purpose of the CCCS is to connect the digital infrastructure of Canadian industry. Parties are not obliged to collaborate with the CCCS. There are, however, ideas to make that happen.

The CCCS publishes a great deal of information on its website. In addition, it distributes threat assessments to parties who have signed a confidentiality agreement for that purpose. Alongside the threat assessments, information classified as TLP AMBER and RED is likewise shared. There is also a Round-Table of cybersecurity companies with which information is shared (similar to the Dutch ISACs). They work with small confidential groups within which discussions are held, for example, on ransomware, and in which organisations share their best practices. Information is also shared with IT infrastructure and cybersecurity companies.

The CCCS has also set up a Cyber Portal where organisations can log in and upload information, which is then analysed by CCCS and, if necessary, the information is shared with others. A distinction is made between two information flows:

1. Service: public information that is distributed to everyone
 2. Information: this can be shared with the organisations registered for that purpose
- Joint analysis mainly takes place with the intelligence services and foreign counterparts such as the US and the UK. At present, no joint analysis takes place with the private sector. However, this is something the CCCS does aim to realise. To achieve this, it will first focus on developing a strategy on how public-private partnerships should be organised, for which purpose it is looking at the i100 in the UK and other initiatives.

Denmark – CFCS

The national CSIRT of Denmark is the Centre for Cyber Security Denmark (CFCS²³), which forms part of the Danish security services. Public-private partnerships in the area of cyber threats and attacks are carried out by CFCS. CFCS works on maintaining the resilience of society through ongoing open/public communication and by way of a structured dialogue on regulated forums.

The Strategic Forum for cooperation in cybersecurity was established in 2014 and is managed by CFCS. The purpose of the forum is to strengthen resilience, with an emphasis on the digital critical infrastructure in Denmark. This is achieved by the forum through the exchange of knowledge between CFCS and industry stakeholders

²² <https://cyber.gc.ca/en/>

²³ <https://www.cfcs.dk/en/>

(IT/telecom, finance, energy, transport and defence sectors), who are invited to participate in the forum by CFCS. The forum meets several times a year.

The members of the forum bring unique knowledge, needs and industry perspectives to the table and thereby add value and increase the level of understanding and knowledge of CFCS. On the other hand, participating organisations also benefit from the expertise and insights of CFCS.

The forum is comparable to the Dutch ISACs. In the Netherlands, this form of public-private partnership has already taken shape.

France – ANSSI

The French national CSIRT is the Agence National de la Sécurité des Systèmes d'Information (ANSSI²⁴). An important goal of the ANSSI with regard to public-private partnerships is to develop a premium community and trusted community. ANSSI wishes to share knowledge and information within this ecosystem, with a focus on companies that provide SOC services, incident response, pen testing and consultancy services (on risk management, technology).

The ANSSI works very closely with cybersecurity companies. The ANSSI has been certifying these companies since 2014 and the ANSSI uses the companies to make critical national infrastructure more resilient as well as to provide incident response services. The ANSSI's approach to public-private partnerships is also more pragmatic than the method used in the Netherlands. For example, a quick start was made with setting up the Campus, without a lengthy consideration of the (legal) framework conditions beforehand. The negative effect of this has been that cohesion within the system, common goals and framework conditions (such as legal aspects) are still largely lacking.

ANSSI is also lacks good technical facilities to share information and knowledge quickly, with many information flows taking place by email or through the ANSSI's informal network. Furthermore, there is no physical platform where organisations (including cybersecurity companies) are able to come together to share or jointly analyse information. The Cyber Campus was set up in January 2022 to organise this (see below).

France – Cyber Campus

The Cyber Campus²⁵ is a large campus (one building in Paris) where many public and private sector organisations come together. It is an initiative that is supported by President Macron. Within the Campus building itself, the companies work on their day-to-day activities. However, there is an explicit desire on their part to collaborate on various cybersecurity issues. In addition to the dedicated spaces for the organisations themselves, collaboration spaces have been set up for this purpose.

²⁴ <https://www.ssi.gouv.fr/en/>

²⁵ <https://campuscyber.fr/en/>

There are also central areas (available for a fee), such as large halls for presentations, and a VIP area has been set up on the roof with restaurant facilities and a roof terrace with a view of the Paris skyline that can be used for events.

More than 100 organisations are currently involved in the Cyber Campus and they collaborate on a wide range of issues on a daily basis. There are 4 key themes within the Cyber Campus (with corresponding goals):

1. Education. Aimed, among other things at recruiting more women into this sector.
2. Operation. This primarily relates to information sharing to increase digital resilience.
3. Innovation. This theme primarily involves new technologies, such as new forms of crypto, etc.
4. Mobilisation. This theme aims to bring all key parties together, including at a European level.

Some 23 foreign public and private partners (including organisations outside Europe) also operate within the Cyber Campus. The management of the campus, however, only includes French or European public/private parties. The campus works with 188 participants from 108 organisations. Its strength is the diversity of the companies ranging from small to big and from public to private.

The building of the Cyber Campus consists of 40 compartments with so-called work spaces. The work takes place in these work spaces with all the organisation involved. The focus of the Campus is also on attracting new organisations and talent.

Commitment is organised through individual financial contributions and through manpower (the representative). Everyone wants to be part of the Cyber Campus because the network is so large and the threshold for participation is low.

United Kingdom – CISP

NCSC-UK²⁶ is the national CSIRT of the United Kingdom and is part of the Government Communications Headquarters (GCHQ). NCSC-UK manages CISP, the Cybersecurity Information Sharing Partnership²⁷. CISP is a joint public and private sector initiative and was set up to allow British organisations to share information on cyber threats within a safe and confidential environment. NCSC-UK is the driving force behind this platform.

Within CISP, some 9000 participants with a range of different backgrounds operate within the platform, such as cybersecurity companies, public sector parties, multinationals, as well as schools with an IT team. Due to the high number of participants, reciprocity is low, as is confidentiality – it is not a trusted community. In addition, there are only a few hundred users that are actually active on the platform.

²⁶ <https://www.ncsc.gov.uk/>

²⁷ <https://www.ncsc.gov.uk/section/keep-up-to-date/cisp>

The platform is managed by a manager who has a background in knowledge sharing and platforms. This was a conscious choice. The platform is entirely geared towards reaching the widest possible target group with the information from the NCSC-UK.

United Kingdom – i100 programme

In addition to CISP (primarily knowledge and information sharing), the United Kingdom also has the i100 programme²⁸ – a smaller cell in which private sector parties collaborate with NCSC-UK. These persons are recruited on the basis of vacancies posted by NCSC-UK and are selected based on a personal profile and based on the organisation they work for, after which they work for NCSC-UK part time, for instance 1 day a week or less.

In practice, there are now some 25 individuals from the private sector working in this programme. NCSC-UK does not have any more available capacity. A system has been set up within the NCSC-UK in which the various departments can ask questions for which the participants in this programme can help find answers through so-called tasks. These questions may relate to specific threat intelligence, but may also be about malware analysis. The people in the programme subsequently look at what information is available within their own organisation that can be shared.

In reality, there is virtually no joint analysis component. NCSC-UK uses the information for its own analyses, which are subsequently shared more widely, i.e. through CISP.

The advantage of i100 is that there is a high degree of confidentiality due to the system of affiliates per organisation. There is also a high degree of commitment due to the fact that these individuals applied for the position themselves.

²⁸ <https://www.ncsc.gov.uk/section/industry-100/partners-and-projects>

OVERVIEW OF DOMESTIC INITIATIVES IN OTHER DOMAINS

CT Infobox

The CT Infobox is a partnership between the AIVD, MIVD, the national police, KMar, the Immigration and Naturalisation Service (IND), the Fiscal Intelligence and Investigation Service (FIOD-ECD), the Public Prosecution Service, FIU-NL, Inspectorate SZW and NCTV, and is part of the AIVD. The purpose of the CT Infobox is to contribute to the fight against terrorism. The CT Infobox brings together information on individuals and networks that are involved in terrorism. After the organisations within the CT Infobox have assessed this intelligence, a review is carried out as to what measures can be implemented and should be taken. This includes criminal justice, immigration or disruption measures. The CT Infobox subsequently issues a relevant opinion and recommendations to the participating parties. As is the case for the CIIC, the employees of the CT Infobox fall under the Wiv regime.

Given that the CT Infobox has been around for several years, there are concerns about its long-term effectiveness, as a result of the 'novelty' of the initiative having worn off. A review is currently under way with all partners involved as to how this can be resolved. The type of participant is crucial to the proper functioning of the CT Infobox. Not every organisation has an interest in sharing or receiving information.

The governance of the CT Infobox is conducted through the coordinating council (legal and administrative/policy), particularly when it comes to formal decisions. Decision making within the CT Infobox could potentially be faster and this is required due to the content of the work.

Due to the confidentiality of the information, information from the CT Infobox is released through an official notice, making it impossible for the origin of the information to be traced.

ECTF

The ECTF is a partnership that focuses on tackling digital crime, primarily in the financial sector. Four major banks, a credit card issuer, the Public Prosecution Service and the police participate in the ECTF. The purpose of the ECTF is to address digital crime and fraud, with phishing forming a key issue within that remit. The partnership was initiated by the Ministry of Security and Justice in 2011 (headed by Minister Ivo Opstelten): a voluntary agreement or covenant was drawn up and signed by all parties. The ECTF primarily focuses on intelligence, investigations and interventions. In practice, each bank contributes 1 FTE and the police have made 5 FTEs available. Within the operational team, both public and private sector parties can initiate investigations.

A supervisory committee steers the operational team and all participants have a representative at tactical/strategic level. They determine the themes within which the ECTF operates.

In order for the ECTF to be effective, it is vital for personal data to be shared and processed. Due to the advent of the GDPR, ECTF was dialled back from 5th to 1st gear due to the fact that this information could no longer be shared. Prior to the advent of the GDPR, the lead time for information sharing was 2/3 hours, after it, it was 3 to 4 weeks (due to requests).

RIEC and LIEC

The ten RIECs²⁹ and the LIEC focus on tackling subversive (organised) crime. They connect the information, expertise and strengths of the various government agencies. In addition, the RIECs and LIEC stimulate and support public-private partnerships in addressing subversion. For example, the initiatives focus on increasing awareness in government and among private sector parties of the subversion issue, strengthening cooperation within the government and with public-private parties and on sharing knowledge and expertise in the area of addressing subversion. The LIEC creates the link between the RIECs and the national partners in addition to which the LIEC provides coordination for crime issues that transcend the region(s).

The RIECs and LIEC support collaboration between various partners, such as municipalities, provinces, the Public Prosecution Service, the police, the Tax and Customs Administration, Dutch Customs, FIOD, etc. Currently, this mainly relates to collaboration with public sector parties, however, ultimately the goal is to establish public-private partnerships.

At present, the RIECs and LIEC are mainly affected by the privacy law aspects involved with the exchange of information. Due to the absence of a legal basis, only a limited exchange of information is currently taking place. This is expected to be resolved when the Wgs comes into effect.

The RIECs and LIEC use phenomenon tables to draw up phenomenon analyses and a strategic knowledge centre has also been set up in which action frameworks are drafted for parties such as municipalities.

²⁹ <https://www.riec.nl/>

ORGANISATIONS CONSULTED

Public organisations

- General Intelligence and Security Service of the Netherlands (AIVD)
- Government Chief Information Officer (CIO-Rijk)
- Cyber Intel/Info Cel
- Digital Trust Centre (DTC)
- Military Intelligence and Security Service (MIVD)
- National Cyber Security Centre (NCSC)
- The National Coordinator for Security and Counterterrorism (NCTV)
- National Police
- Public Prosecution Service
- Legislation and Legal Affairs Department (Ministry of Justice and Security)

Private organisations

- ATOS NL
- Capgemini
- Chapter8
- NL CISO Circle of Trust (CCoT)
- Conclusion
- Deloitte
- ECP | Platform voor de Informatiesamenleving
- ECTF
- Fujitsu
- FOX-IT
- IBD
- KPN
- National Information and Expertise Centre (LIEC)
- Dutch Security Hotline (Nationaal Security Meldpunt)
- NFIR
- Northwave
- NXP
- SHV
- Surf-Cert
- Teambblue
- T-Mobile
- VNO-NCW
- Z-CERT

Academia

- ACCSS (ACademic Cyber Security Society)
- Prof.dr. B. van den Berg, Leiden University
- Prof.dr. E.H. Klijn, Erasmus University Rotterdam
- Prof.dr. B.W. Schermer, Leiden University

LIST OF ABBREVIATIONS

AAN	Anti Abuse Network
ABDO	General Security Requirements for Defence Contracts
ABRO	General Security Requirements for Central Government Contracts
AIVD	General Intelligence and Security Service of the Netherlands
ANSSI	Agence Nationale de la Sécurité des systèmes d'information
GDPR	General Data Protection Regulation
CCCS	Canadian Center for Cyber Security
CERT	Computer Emergency Response Team
CFCS-Denmark	Centre For Cyber Security Denmark
CIIC	Cyber Info/Intel Cel
CISO	Chief Information Security Officer
CISP-UK	Cybersecurity Information Sharing Partnership United Kingdom
CMMI	Capability Maturity Model Integration
CSE	Communication Security Establishment (Canadian intelligence services)
CSIRT	Computer Security Incident Response Team
CT	Counterterrorism
DIVD	Dutch Institute for Vulnerability Disclosure
DPIA	Data Privacy Impact Assessment
DSP	Digital Service Provider
DTC	Digital Trust Centre
ECD	Economic Investigation Service
ECTF	Electronic Crimes Task Force
FIOD	Fiscal Intelligence and Investigation Service
FIU	Financial Intelligence Unit
IOC	Indicator of compromise
IPS	Internet Service Provider
ISAC	Information Sharing and Analysis Centre
KMAR	Royal Netherlands Military Police
LDS	Nationwide Network of Information Exchanges
LIEC	National Information and Expertise Centre
MISP	Malware Information Sharing Platform
MIVD	Military Intelligence and Security Service
MO	Modus Operandi
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
N-CERT	National Emergency Response Team
NCSA	National Cyber Security Agenda

NCSC	National Cyber Security Centre
NCTV	National Coordinator for Security and Counterterrorism
NDN	National Detection Network
NIS2	Network and Information Security Directive version 2
OKTT	Objective manifest duty (to inform the wider public)
OT	Operational Technology
PGP	Pretty Good Privacy
RIEC	Regional Information and Expertise Centre
SIEM	Security Incident and Event Monitoring
SOC	Security Operational Centre
Stg	State secret
STIX	Structured Threat Information Expression
Tip	Threat Intelligence Platform
TLP	Traffic Light Protocol
VSSR	Government SOC System Enhancement Programme
Wbni	Network and Information Systems Security Act
Wgs	Data Processing by Partnerships Act
Wiv	Intelligence and Security Services Act 2017
Wpg	Police Data Act