Annex 6 of the Cyber Resilience Network (CRN) Construction Plan

Caribbean part of the Kingdom of the Netherlands

The NCSC’s approach to advancing effective cooperation

9-7-2025

0. Introduction

Between September 2024 and May 2025, the National Cyber Security Centre (NCSC) worked on a plan for the Caribbean part of the Kingdom of the Netherlands (CpKNL). The CpKNL's needs in terms of developing digital resilience are different from those of the Netherlands. This necessitated the adoption of an alternative approach.

This plan is part of the Cyber Resilience Network (CRN) construction plan and has been coordinated with the various policy departments and implementing organisations involved. It provides a structured framework for the approach to constructing a Cyber Resilience Network in the CpKNL that takes full account of the local context.

1. From initiatives to networks

A policy decision has been made to extend the Cyber Resilience Network across the entire Kingdom of the Netherlands. A broad set of network partners needs to be actively sought to facilitate this as part of a joint effort.[1] New network partners are therefore being recruited for the Cyber Resilience Network. They include providers of ICT and security services that play an important role in making organisations resilient.

In the Caribbean region, there is a heightened focus on digitisation, accompanied by increased attention to cyber security and digital resilience. In the absence of designated critical companies in the region, there remains no legal obligation for key sector entities, such as energy, water and telecom companies, to implement specific measures. Support for businesses is still lacking, and collaborative engagement is limited. Matribu B.V.'s project titled 'Strengthening Cyber Resilience in the Caribbean Netherlands' (*Versterken Cyberweerbaarheid Caribisch Nederland*) is changing this by offering low-threshold cyber security scans and establishing an ISAC network. This represents a starting point towards analysing and strengthening business resilience in that part of the Kingdom. In December 2024, the project was awarded the 'Strengthening Cyber Resilience' subsidy. The Digital Trust Center (DTC) is the sponsor of the subsidy, with responsibility for subsidy implementation assigned to the Netherlands Enterprise Agency (RVO).

There is currently no framework of systematic consultation between the Netherlands and the CpKNL . Within the entire Kingdom, the Cyber Resilience Network could assume a facilitating role in connecting the network with the ultimate aim of phasing in a public-private partnership. This phased approach differs in various respects from the construction of the Cyber Resilience Network in the Netherlands (see Annexes 1, 2 and 3). More time will be allocated to building the Cyber Resilience Network with and within the CpKNL, with an initial focus on development in the Caribbean Netherlands[2]. Once the first steps have been taken there, consideration will be given to the set-up and cooperation with the autonomous countries. The lead-up to this is structured into four distinct phases:

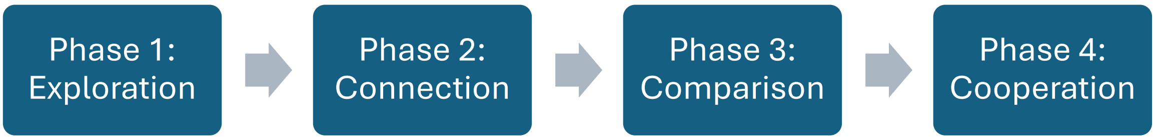

Figure 1. Four stages of establishing the network

Phase 1: Exploration

Phase 1 will be devoted to a broad exploration with the organisations and stakeholders involved. It will provide an insight into the current cyber domain, existing partnerships and initiatives, wants and needs, risks and dependencies, cyber resilience in the CpKNL and key local network partners. The starting point is that the Cyber Resilience Network should provide the same capabilities for the CpKNL as for the rest of the Kingdom. With both the special municipalities and the autonomous countries taking part, there are inevitably differences in laws and regulations[3]. All forms of collaboration and exchange within the Cyber Resilience Network must, of course, be in line with the applicable laws and regulations.

At this point, we are already in phase 1. A start has been made on identifying the network partners. This initial exploration, which proceeds from the Cyber Resilience Network, is focused mainly on Bonaire and

[1] Vision for the Cyber Resilience Network, p. 41.

[2] See Annex A for constitutional relationship; the Caribbean Netherlands consists of the BES islands (the islands of Bonaire, Sint Eustatius and Saba. Autonomous countries are the CAS countries (Curaçao, Aruba and Sint Maarten).

[3] The autonomous countries have their own laws and regulations. As regards the Public Entities, parts of old Antillean legislation have been modernised, and in some cases European Dutch laws also apply to the Caribbean Netherlands, an example being the Digital Resilience of the Business Community (Promotion) Act (*Wet bevordering digitale weerbaarheid bedrijven*).

is therefore not representative of the entire CpKNL. It is advisable to broaden this exploration first to include the other islands in the Caribbean Netherlands, and then to the autonomous islands. In this phase, there should be attention to and information on local circumstances, the socio-cultural context and the current situation. For instance, careful consideration should be given to the differences in culture, behaviour, expertise and available capacity and resources in the CpKNL compared with the Netherlands. In addition, greater insight is required into existing collaborations - to the extent there are any - so that they can be included in the Cyber Resilience Network in an appropriate manner and work can be jointly undertaken towards establishing a realistic understanding of the current status of cyber resilience in the CpKNL.

Phase 2: Connection

The outcomes of the exploration phase will be used in phase 2, the connection phase. It is important to connect network partners and jointly analyse the results of the exploration phase. This will make it possible to identify and prioritise the key cyber resilience themes. These themes form the basis for partnership within the Cyber Resilience Network. This phase will be carried out in a setting that allows network partners to collaborate in confidence, share knowledge and provide feedback.

Phase 3: Comparison

Phase 3 will start with the themes prioritised in phase 2. They will form the basis for defining the desired situation. Based on an analysis of strengths and weaknesses (gap analysis), we will then look at what is still needed to achieve this desired situation. The outcomes will be the descriptions of the Cyber Resilience Network functions and the basis for collaboration within the network. As a result of local circumstances, the functions may be different from those in the Netherlands. Ultimately, however, it will be important to seek as much synergy as possible between the CpKNL and the Netherlands in order to make efficient use of the scarce knowledge, resources and capacity within the Cyber Resilience Network.

Phase 4: Cooperation

Phase 4 involves working together on the themes and pillars from phases 2 and 3. Challenges will be shared in confidence and solutions sought in the network. A tailored future plan, designed by and for the network partners, is in place to enhance cyber resilience in the CpKNL. The network partners are well connected to Cyber Resilience Networks in both the CpKNL and the Netherlands. They will be able to independently apply the established Cyber Resilience Network's functions and further develop them together.

2. Network map

The network map (Figure 2) is the result of the initial exploration that proceeded from the Cyber Resilience Network, with a focus on Bonaire[4]. It provides an overview of both current and potential network partners and sheds light on mutual relationships and dependencies. Not all organisations shown have been contacted. However, that is desirable for any further exploration. As we are currently still in phase 1, the network map is not yet fully complete and additions will need to be made to it.

[4] This network map provides an initial insight from the exploration that proceeds from the Cyber Resilience Network. Consequently, it does not yet include all network partners, organisations and/or initiatives involving the CpKNL (either in the CpKNL or the Netherlands).

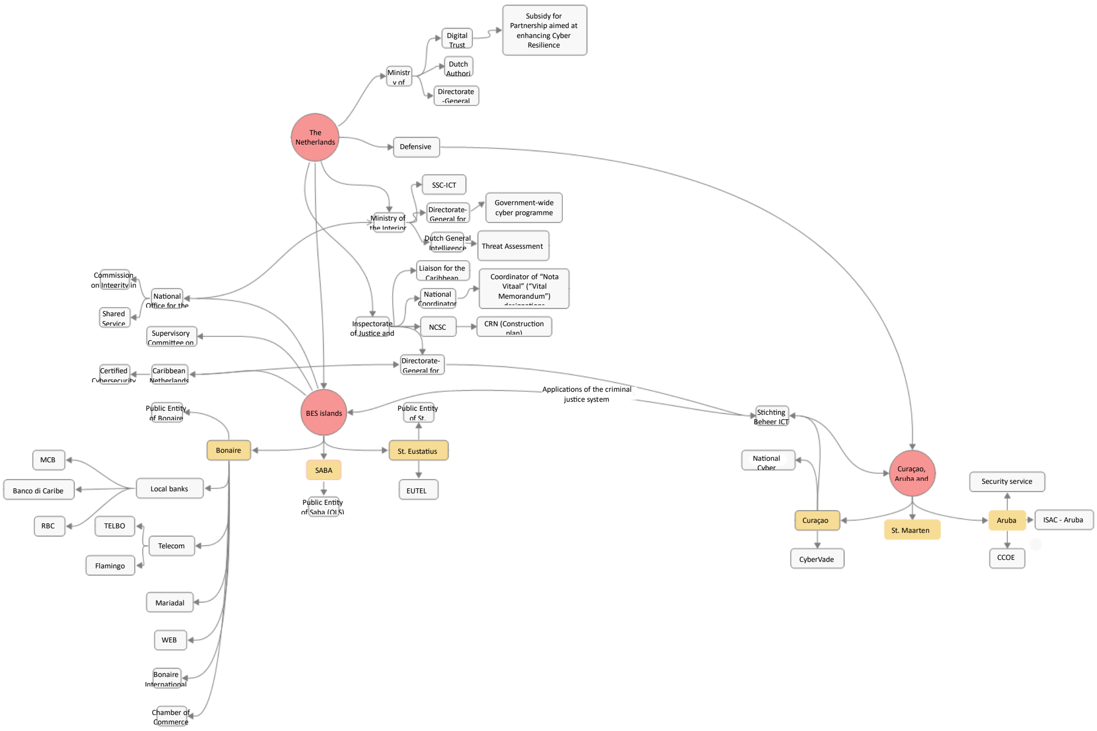

Figure 2: Network map exploration

3. Activities and Deliverables

Phase 1: Exploration		
Activities	**Deliverables**	**Timing and/or phase[5]**
NCSC's identification of network partners for the Cyber Resilience Network - In collaboration with the Ministry of the Interior and Kingdom Relations (BZK), Ministry of Economic Affairs/Digital Trust Center (EZ/DTC) and the Ministry of Justice and Security (JenV), both for the Caribbean Netherlands (which will have the initial focus) and the autonomous countries.	Publication of network map with a list of network partners and the connections between them.	Start of phase 1: - The Caribbean Netherlands: ready Q1-2026: - Autonomous countries: Q1-2027.
Identify relevant initiatives and overlap in conjunction with the NCSC, Ministry of the Interior and Kingdom Relations (BZK), Ministry of Economic Affairs/Digital Trust Center (EZ/DTC) and the Ministry of Justice and Security (JenV) - Both for the Caribbean Netherlands (which will have the initial focus) and the autonomous countries.	Publication list of initiatives (both local and departmental).	Start of phase 1: - The Caribbean Netherlands: ready Q1-2026: - Autonomous countries: ready Q1-2027.
NCSC investigation along with network partners of wants and needs for the CRN - Working session with network partners to identify wants and needs.	Publication of wants and needs in the cyber domain, including a possible problem analysis.	Mid-phase 1: - Caribbean Netherlands: ready Q2-2026:

[5] All the dates mentioned are target dates. Achieving the deliverables within the desired timeframe is dependent on internal and external factors, so the final delivery date may differ from the target date.

- Contributing to and participating in local initiatives (such as the BQ conference). - Both for the Caribbean Netherlands (which will have the initial focus) and the autonomous countries. In collaboration with BZK, EZ and JenV.		• Autonomous countries: Q3-2027.
Risk analysis by NCSC and others (possible inclusion of other involved parties) - Implement (adapted) MASKeR pathway with local network partners. Both for the Caribbean Netherlands (which will have the initial focus) and the autonomous countries. Overarching chains (e.g. SBIR[6], SSO RCN).	Reporting risks and chain dependencies.	Mid-phase 1: • Caribbean Netherlands: ready Q2-2026: • Autonomous countries: Q3-2027.
Report on 'state of the cyber domain in the CpKNL' to be developed by the network - Report on the details of phase 1. - Establishing and consolidating activities carried out in phase 1 to be translated into annual plans/annual calendars. - Details regarding the phases and concrete follow-up steps	Report of the findings obtained in phase 1. Publication of annual activities.	End of phase 1: • Ready Q4-2027.

Phase 2: Connection		
Activities	**Deliverables**	**Timing and/or phase**
Organise/encourage collaborative digitisation and cyber resilience by the network (support from the NCSC and other parties) - Bringing together the network partners identified, where possible by local network partners. - Unifying existing initiatives where possible. Unite network partners in a partnership (possibly by formalising an agreement). In collaboration with BZK, EZ and JenV.	Formalisation of network partners (possibly in a partnership).	Start of phase 2: • Ready Q1-2028.
Identification and prioritisation of collaboration themes by the network (support from the NCSC and other parties) Working sessions to identify and prioritise structured themes in consultation with all network partners involved.	Publication of initial structure of the Cyber Resilience Network functions.	End of phase 2, start of phase 3: • Ready Q2-2028.

Phase 3: Comparison		
Activities	**Deliverables**	**Timing and/or phase**
Identification and prioritisation of collaboration themes by the network (support from the NCSC and other parties) Working sessions to identify and prioritise structured themes in consultation with all network partners involved.	Publication of initial structure of the Cyber Resilience Network functions.	End of phase 2, start of phase 3: • Ready Q2-2028.
Gap analysis by the network (support from NCSC and other parties)	Publication summary of the pillars implementation plan. Cyber Resilience Network and	Mid/end of Phase 3 Long term • Ready Q4-2028.

[6] Stichting beheer ICT-rechtshandhaving

- The network partners make individual gap analyses. - Working sessions to compare the individual gap analyses. Working sessions to compare the gap analyses with the Dutch Cyber Resilience Network.	connection to the Cyber Resilience Network in place in the Netherlands. Connection to the Cyber Resilience Network Community.	

Phase 4: Comparison		
Activities	**Deliverables**	**Timing and/or phase**
The network's future plan of the Cyber Resilience Network for the CpKNL - Detailing of the progress and conclusions reached during the phases. - Successes and attention points. Detailing of activities that have yet to be undertaken in the network. In collaboration with the NCSC, BZK, EZ and JenV.	Publication future. Cyber Resilience Network and the CpKNL.	Phase 4: • Ready Q2-2029.

4. Enabling conditions

Various enabling conditions have been defined to facilitate the conditional inclusion of the CpKNL in the establishment and further development of the Cyber Resilience Network.

Mutual expectations

During the NCSC's initial exploration, it became clear that there are widely differing stakeholders who wish to play a part in enhancing cyber resilience in the CpKNL. That makes for a wide range of ideas, perspectives, wants and needs. Each stakeholder will have its own expectations about the themes, pillars and plans that are to be established and developed. It is therefore important to monitor and discuss expectations with stakeholders in every phase and to decide what can and cannot be realised. Only in this way will they be able to collaborate fully and freely.

Support

The Cyber Resilience Network is a network for and by public and private network partners. For the network to succeed, reciprocity is expected in it. This involves joint investment to increase effectiveness and knowledge in the domain. That said, connecting the CpKNL will be a complex puzzle. To manage this, it is important to provide the right support and guidance to stakeholders in the CpKNL, which will include the specific knowledge and expertise of the Windward Islands. Based on the initial exploration, it is advised that the NCSC offer a supporting role in going through the phases with stakeholders and network partners. Besides iteratively going through the phases, this support will include an assurance of continuity. To achieve this, structural commitment to establishment of the network by the NCSC is necessary. One example of this will be the establishment, guidance and monitoring of working and other sessions. The NCSC's support in further developing the Cyber Resilience Network for the CpKNL will always need to be in coordination with other relevant ministries and implementing organisations, both locally and in the Netherlands. This may also require structural capacity from other organisations. This will need to be determined in due course. As regards sufficient funding for the establishment, specifications and management of the CpKNL's Cyber Resilience Network, chapter 7.3.3 of the Cyber Resilience Network Construction Plan applies.

Planning

Each country/island in the Kingdom of the Netherlands has its own historical influences, traditions and culture. Collaboration on the Cyber Resilience Network and the connection with Dutch network partners are a new development. It is important to take the time to gain insight into the current cyber domain, wants and needs, risks and dependencies described in phase 1. There should also be room for cultural differences and building a cyber community in a way that enables knowledge and experience to be shared. To set this up in a structured manner, it is recommended that the exploration start with the special municipalities and then to include the lessons they have learned in a later exploration with the autonomous countries. It is recommended to spend one year on each of these two explorations.

Interdepartmental cooperation

To ensure that the desired outcomes on digital resilience are achieved, it is important that departments coordinate their activities related to the CpKNL. Programmes and projects could overlap or even get in each other's way. Good communication, interdepartmental cooperation and knowledge sharing are therefore important. There is only limited capacity, expertise and knowledge available in the islands to implement all the Dutch projects and programmes. Departments must guard against overloading local organisations on the same projects and goals. Coordination is therefore necessary. One example would be to concentrate this in a self-managing coordination group that includes representatives from the relevant departments.

Annex A Definition and Scope of the Caribbean part of the Kingdom of the Netherlands

On 10 October 2010, the constitutional relationship between the Caribbean parts of the Kingdom and the Netherlands altered. This resulted in the dissolution of the Netherlands Antilles. The islands of Bonaire, Sint Eustatius and Saba (the BES islands) have since constituted public entities within the country of the Netherlands and are collectively referred to as the Caribbean Netherlands. Curaçao, Sint Maarten and Aruba have become independent countries within the Kingdom of the Netherlands. Following the constitutional changes implemented in 2010, it was agreed that caution should be exercised when introducing new legislation. The main purpose of this was to give citizens and administrators a period of rest and acclimatisation. The coalition government under Prime Minister Dick Schoof is committed to clear and effective prioritisation regarding the activities to be undertaken for the CpKNL, which requires a clear framework for weighing up decisions in that regard. The premise of previous governments regarding efforts facilitating a more equal level of facilities in the Caribbean Netherlands has thus been abandoned.

The countries in the Caribbean region have the status of 'overseas countries and territories' (OCTs). This status refers to non-European countries and territories that have a special relationship with the Netherlands. The term “non-European” means that those countries are not part of the territory of the European Union. Therefore, laws and regulations that apply to the European territory, including the NIS2 Directive, do not automatically apply to the Caribbean Netherlands. The Netherlands has chosen not to implement the NIS2 Directive for public entities. As a result, the Caribbean Netherlands has no cyber legislation. The autonomous countries similarly have no cyber legislation in place. The General Data Protection Regulation (GDPR) also does not apply to the Caribbean Netherlands. The autonomous countries have their own national ordinances. Curaçao and Sint Maarten each have a national ordinance on personal data protection. Aruba has a ‘National Ordinance Person Registration’. Protection of personal data is regulated for the public entities in the BES Personal Data Protection Act (*Wet bescherming persoonsgegevens BES*). The autonomous countries have their own laws for the protection of privacy and personal data.

Changes may be made to the CpKNL’s cyber laws and regulations. Action line 7 of the Security Strategy for the Kingdom of the Netherlands states: ‘Strengthening digital resilience’ is the following priority for the years 2023-2029: ‘Constructing cyber security policy for the CpKNL. Legislation and policy frameworks are needed to promote cybersecurity and counter cybercrime, important elements of which are enhanced knowledge sharing, cooperation and technical assistance between the Netherlands and CpKNL. In addition, greater effort is needed to increase cyber awareness, implementation of cyber security policies, and technical expertise, both among citizens and in the public and private sectors’[7].

[7] ‚Security Strategy for the Kingdom of the Netherlands | Publication | National Coordinator for Counterterrorism and Security

Annex B. The Cyber Resilience Network and overlaps with other initiatives in the Caribbean part of the Kingdom

Although most Dutch cyber laws and regulations do not apply to the CpKNL, there are several policy and other initiatives that affect the Caribbean part of the Kingdom as well.

The Digital Resilience of the Business Community (Promotion) Act (Wbdwb), which entered into force on 1 October 2024, does apply, albeit only in the Caribbean Netherlands. This law defines the tasks and powers of the Minister of Economic Affairs (EZ) as regards the digital resilience of non-critical companies in the Netherlands, such as regarding the dissemination of information on vulnerabilities, threats and incidents, and promoting cooperation within the business community in terms of digital resilience.

On 4 November 2022, *the* Value-Driven Digitisation Work Agenda (*de* Werkagenda Waardengedreven Digitaliseren), which also touches on cyber resilience in the Caribbean region of the Kingdom of the Netherlands, was presented to the House of Representatives. Conclusions in that regard were drawn in December 2023.[8]. The Work Agenda is an elaboration of elements from the letter titled Main Points of Digitisation Policy (*Hoofdlijnen Beleid Digitalisering*)[9], and sets out concrete goals and actions. It includes five pathways: participation, trust and guidance in digital society, good digital government and strengthening digital society in the CpKNL. It is updated annually.

Efforts include strengthening digital security and resilience. At a time when the world around us is unsettled, security is critical. Using the Ministry of Justice and Security's cybersecurity strategy as a guiding tool, work has been undertaken to strengthen digital security and resilience. For example, the Revised EU Network and Information Security Directive raised the basic standard for organisations. Simultaneously, efforts were made to develop appropriate support structures and mechanisms. Examples include the creation of tools to help government organisations procure ICT products and services securely and the development of a government-wide red teaming initiative to detect infrastructure weaknesses as early as possible.[10]

In its work agenda, the Cabinet Digitisation Policy expresses its desire to strengthen digital society in the CpKNL[11]. Its aims are:

1. **Digital optimisation** so that everyone in the Caribbean Netherlands has access to sufficient knowledge, services and facilities to take advantage of opportunities and adequately mitigate risks.
2. **Collaboration on the digital basics** with society, businesses and the governments of Aruba, Curaçao and Sint Maarten to ensure that they too are adequately equipped.

The Cabinet Digitisation Policy sees in the action plan the challenges that exist in international connectivity, both in the Caribbean region and between that region and Europe.[12]

Where possible, the aim of Cyber Resilience will be to connect and further strengthen these existing cyber resilience initiatives in the CpKNL. This will be further explained in the following chapters.

[8] The Work Agenda: one year on - Value-Driven Work Agenda on Digitisation - Digital Government

[9] Letter to the House of Representatives setting out the main points of digitisation policy | Parliamentary Document | Rijksoverheid.nl

[10] The Work Agenda: one year on - Value-Driven Work Agenda on Digitisation - Digital Government

[11] 5. Strengthening digital society in the Caribbean part of the Kingdom of the Netherlands; Strengthening digital society in the Caribbean part of the Kingdom of the Netherlands - Digital Government

[12] 5.2 Collaborating on digital society within the Kingdom of the Netherlands; Strengthening digital society in the Caribbean part of the Kingdom of the Netherlands - Digital Government

Annex C. Current situation

In spring 2024, work began on fulfilling the next objective of the Netherlands Cybersecurity Strategy (NLCS): 'An exploration of the steps needed to increase the digital resilience of critical infrastructure in the Caribbean Netherlands will be initiated.' The NCSC began this exploration, which resulted in the initial conclusions and subsequent objective(s). The current state of play is the result of discussions with organisations in the Caribbean region and collaboration with the Ministry of the Interior and Kingdom Relations, the Ministry of Economic Affairs and the Ministry of Justice and Security.

1. Initial exploration and conclusions

The aim to increase and improve the CpKNL's inclusion in cyber developments and cyber resilience is in line with the developments of the Cyber Resilience Network. The exploration reveals that leaders of critical organisations are looking for guidance and frameworks to come together and thus to increase cyber resilience. Tentative steps have already been taken to establish partnerships. In addition, cross-sectoral exploratory discussions on cyber resilience have already taken place. However, these are not (or not yet) of a structural nature. Added to this, the cultural context does not facilitate cooperation with other islands and the Netherlands. Also, there is a great need for a better connection to technical and operational knowledge, capacity in the form of personnel and assistance from the Netherlands (including in the form of responses), but also an understanding of the maturity of the cyber domain as well as exercises and training.

Specifically, there is a need for coordination and a plan of action to embed digitisation and cyber resilience. An initial step in this regard is to improve awareness and urgency of the matter among critical organisations. Critical organisations can then access technical products and services in the Netherlands. From that point, public-private partnerships can be phased in to develop the Cyber Resilience Network. However, it is imperative that organisations recognise the importance of this and make capacity available. This sequencing will ensure that products and services are in line with the current policies of critical organisations in the islands.

2. Exploration of the Caribbean Region

Ministry of the Interior and Kingdom Relations

The Ministry of the Interior and Kingdom Relations works on the basis and core value of democracy for both the Netherlands and the CpKNL. In addition, it supports the autonomous countries of Aruba, Curaçao and Sint Maarten in building a strong foundation for a good life. It also provides support for the public entities' cyber resilience.

The Ministry has two main information security tasks in the Caribbean Netherlands:

- **System responsibility**: Ensuring the security of government information in all parts of the Kingdom.
- **Contracting authority for projects**: Adopting the active role of contracting authority for digitisation projects and, in that role, setting an example in terms of safe working practices.

Work is currently being done on planning the implementation of the Ministry's main tasks. The Ministry is holding talks with public entities and other relevant partners in the Caribbean Netherlands. The primary focus is on gaining an accurate picture of cyber resilience and the challenges involved. The Ministry is also launching projects to assist public entities in the field ofcyber resilience. One aim of this will be to connect with the Cyber Resilience Network. In addition, the Caribbean Netherlands will be involved in the government-wide cyber exercise which the Ministry organises every year.

Topics currently being addressed from part of the Ministry's planning:

- Coordination, baselines and insight
- Working on relationships and trust
- Awareness and technical training
- Cybersecurity Community Building
- Sectoral CSIRT and Incident Response
- Crisis management

Ministry of Economic Affairs

The Ministry of Economic Affairs is working to establish a sustainable and entrepreneurial Caribbean Netherlands. It also contributes to sustainable economic growth by ensuring reliable utilities. The Ministry is helping the islands improve the value for money of telecom and internet services by defining frameworks and providing subsidies. The Digital Economy Strategy - Progress Report 2024 includes the following goal: 'Strengthening the Caribbean Netherlands' digital infrastructure in order to improve quality, reliability and affordability[13]. 'This strategy also includes reference to the Digital Trust Center (DTC) and the Cyber Resilience Subsidy Scheme. The DTC is a department of the Ministry of Economic Affairs. The DTC's mission is to support over two million Dutch companies - from self-employed professionals to large corporations - to improve their resilience against increasing cyber threats. These are all businesses in the Netherlands that operate in the non-critical sectors. Working under the responsibility of the Minister of Economic Affairs, the DTC implements the Digital Resilience of the Business Community (Promotion) Act, which entered into force on 1 October 2024 (see also Annex A). In addition, the Ministry's publication titled 'the State of the Digital Infrastructure' (SDI) includes a chapter on digital infrastructure in the Caribbean Netherlands, which also deals with resilience. Along with the SDI, a report on digital infrastructure in the Caribbean Netherlands was sent to the House of Representatives[14].

Ministry of Justice and Security

The Ministry of Justice and Security ensures that the rule of law is safeguarded in the Caribbean Netherlands so that people can live alongside each other in freedom, regardless of lifestyle or opinion. The following departments and services operate in the Caribbean Netherlands under the Ministry's responsibility: The Caribbean Netherlands Police Force, Fire Service, Victim Support Centre, Netherlands Caribbean Correctional Institution, Public Prosecution Service, Probation Service, Free Legal Assistance, Netherlands Caribbean Immigration and Naturalisation Service, Guardianship Council and the Violent Offences Compensation Fund.

The Netherlands' government has drawn up a Security Strategy for the Kingdom of the Netherlands which also aims to ensure the security of the Caribbean Region.[15] The document deals with various matters including cyber threats against the Kingdom. The strategy states: 'The CpKNL has also been subjected to cyber attacks with potentially socially disruptive consequences. One example was the major ransomware attack on Sint Maarten's only water and electricity utility in 2022. It caused the company to lose access to its financial data and no recent backup was available. This posed a threat to the operations and continuity of two vital services: water and electricity.' Action line 7 discusses strengthening digital resilience, formulating a cybersecurity policy for the CpKNL and strengthening cooperation between the Netherlands and the Caribbean part of the Kingdom. This should include efforts to raise cyber awareness as well as implementing cyber security policies and technical expertise. Action line 12 discusses strengthening crisis

[13] Strategie Digitale Economie - Voortgangsrapportage 2024

[14] Staat van de Digitale Infrastructuur - Tweede Kamer 2023-2024, 26643 nr 1119

[15] Veiligheidsstrategie voor het Koninkrijk der Nederlanden | Rapport | Rijksdienst Caribisch Nederland

management and increasing community preparedness. It also focuses on improving information sharing and crisis plans, with an emphasis on giving greater consideration to local context and autonomy.

Currently, organisations do not qualify for critical status because the relevant guidelines are based on Dutch standards. The National Coordinator for Security and Counterterrorism (NCTV) is now investigating possible solutions in consultation with the Ministry of the Interior and Kingdom Relations, the Ministry of Economic Affairs and the NCSC. The expected timeline is not yet known.

The NCSC has had occasional contact with organisations in the CpKNL in recent years. It is not yet clear what products and services the NCSC is allowed to provide to CpKNL. Current legislation does not provide any basis for providing structural operational support and information sharing with organisations in the CpKNL. That said, in recent years the NCSC has been working with organisations in the CpKNL to look at what is possible. The exploration proceeding from the Cyber Resilience Network marks the beginning of establishing a structural basis and relationship with critical organisations in the CpKNL.