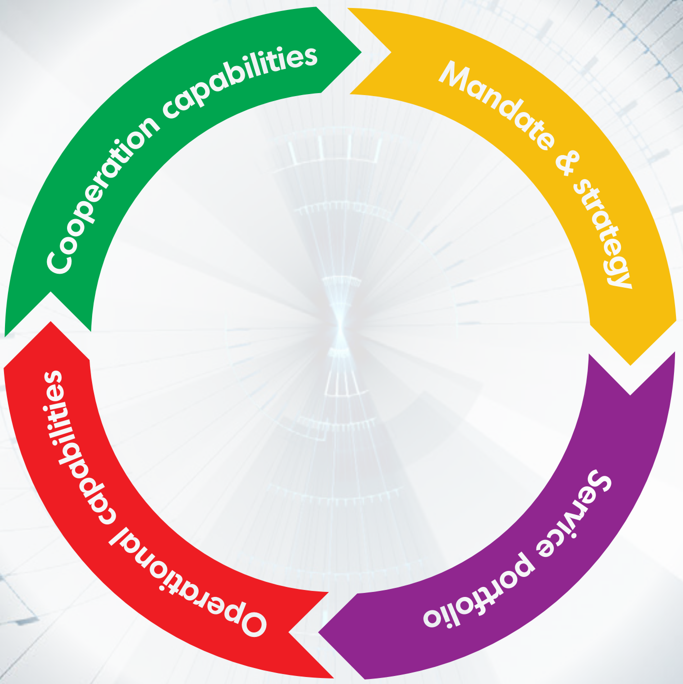
enisa
European Network
and Information
Security Agency

Updated Recommendations 2012

Baseline Capabilities of National/Governmental CERTs



Document History

Date	Version	Modification	Author
December 2009	1.0 initial draft	Baseline Capabilities of National/Governmental CERTs Part 1: Operational Aspects	ENISA
December 2010	1.0 initial draft	Baseline Capabilities of National/Governmental CERTs Part 2: Policy Recommendations	ENISA
October 2012	2.0	Deployment of Baseline Capabilities of National/ Governmental CERTs: Status Report 2012	ENISA
October 2012	2.0	Baseline Capabilities of National/Governmental CERTs: Updated Recommendations 2012	ENISA

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as lastly amended by Regulation (EU) No 580/2011. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Contact details

To contact ENISA for this report please use the following details:

Email: opsec@enisa.europa.eu

Internet: http://www.enisa.europa.eu

Contributors to this report

We would like to thank our ENISA colleagues who contributed with their input to this report and supervised its completion:

Contributors and Editors – Andrea Dufkova, Silvia Portesi and Romain Bourgue;

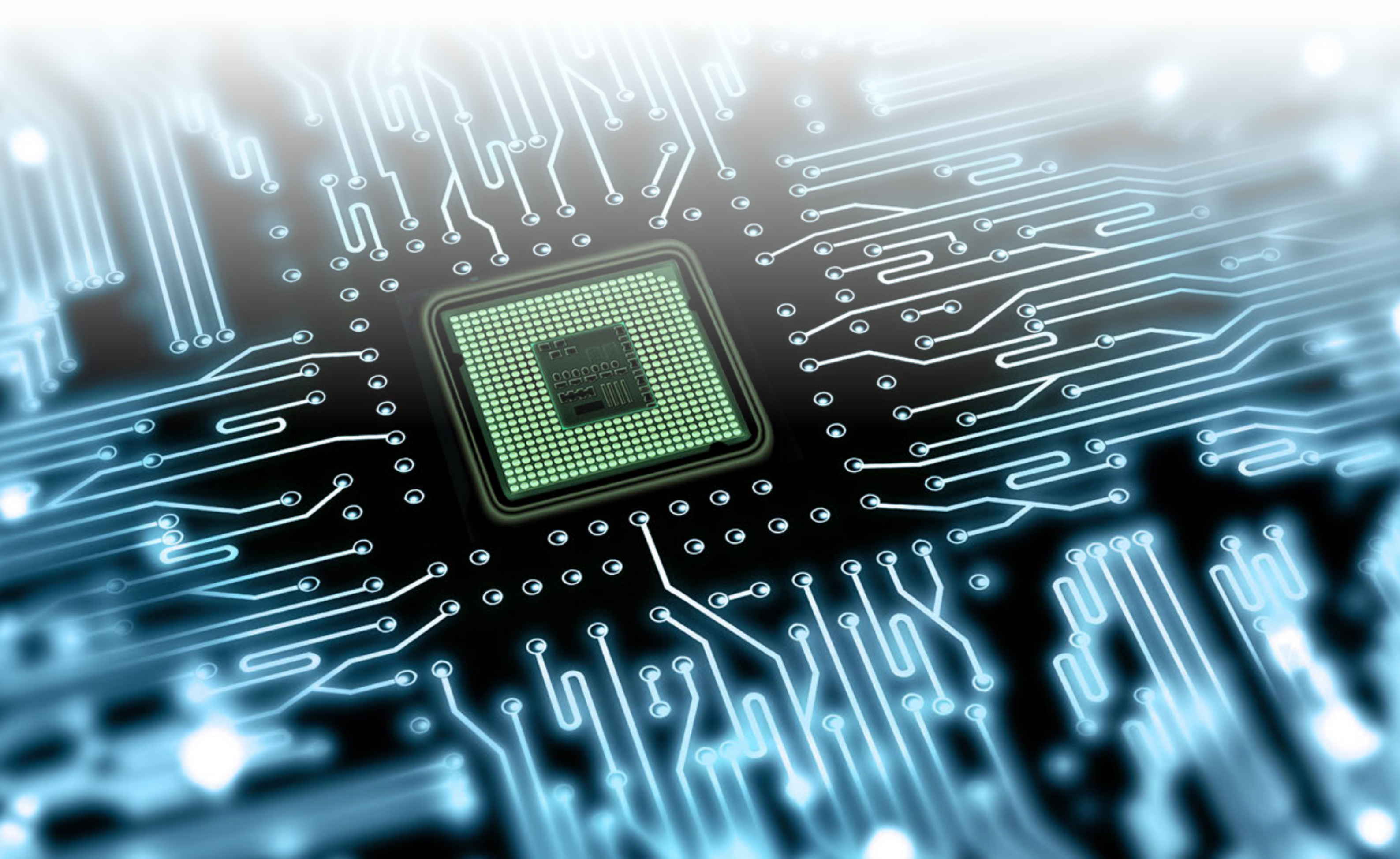
Reviewers – Lauri Palkmets, Jo De Muynck, Konstantinos Moulinos and Thomas Haeberlen.

We would also like to thank the study team from IDC CEMA, commissioned by ENISA to undertake the study, in particular Joshua Budd, Jachym Homola and Matthew Marden.

Acknowledgements

We would like to thank all the 45 stakeholders across Europe who provided their inputs for this report in the form of returned surveys and/or subsequent interviews. We very much appreciate the active involvement of the national/governmental CERTs as well as the contributions of other CERTs, policymakers in the area of cyber-security, regulators, operators and other stakeholders.

Our special thanks go to the members of the Informal Expert Group established by ENISA, who provided feedback to this report. The members include: Todor Dragostinov (CERT Bulgaria), Marcos Gomez Hidalgo (INTECO), Stefan B. Grinneby (CERT-SE), Brian Honan (IRISS-CERT), Petra Hochmannová (CSIRT.SK), Jaroslav Janáček (Comenius University), Andrea Kropáčová (CSIRT.CZ), Otmar Lendl (CERT.AT), Monica Pellegrino (ABI Lab), Stephen Sheridan (ETHZ-NSG) and Dan Tofan (CERT.RO).



Contents

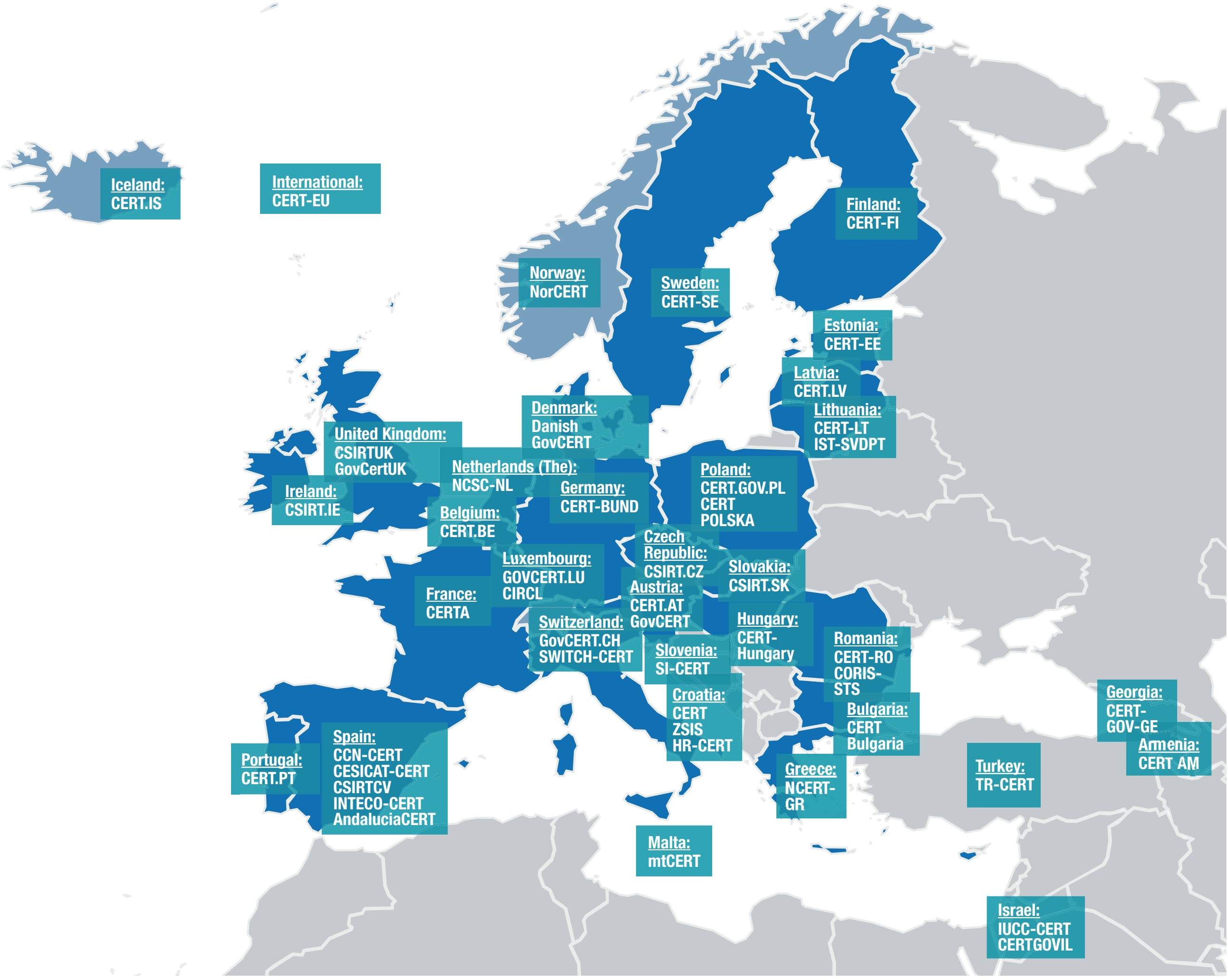
List of Figures

1

Executive summary

1 Executive Summary

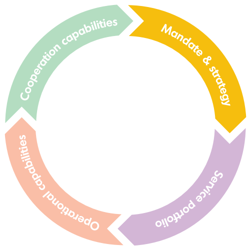
The aim of this report is to deliver an updated set of recommendations on baseline capabilities for national/governmental CERTs[1] (Computer Emergency Response Teams) in Europe. ENISA drafted the original recommendations in 2009/2010.[2] Based on the assessment of deployment of baseline capabilities (see the accompanying report 'Deployment of Baseline Capabilities of National/governmental CERTs – Status Report 2012') ENISA has identified a number of gaps and shortcomings that still need to be addressed in order for n/g CERTs to fully meet their baseline capabilities. The gaps are outlined in this report along with recommendations on how to address them. In line with the original document, all four n/g CERT capabilities are covered: mandate and strategy, service portfolio, operation and cooperation.



[1] A Computer Emergency Response Team (CERT) is a team of IT security experts whose main business is to respond to computer security incidents. The team provides the necessary services to handle such incidents and to support their constituents (the established term for their customer base) to recover from computer security breaches. In order to mitigate risks and minimise the number of required responses, most CERTs also provide preventative and educational services for their constituency.

[2] http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities

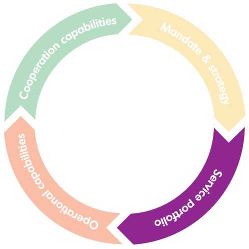
1. Executive Summary



Mandate and Strategy

Regarding the mandate of n/g CERTs, there remains a **permanent need for clarification** so that they can support all the activities carried out by n/g CERT teams. For reasons of transparency, Member States also have to ensure that the mandate is made public and communicated properly. In the mandate, the **role and responsibilities of the governmental CERT type** including funding provisions **should also be specified** in order to remove doubts associated with responsibilities and funding of the CERTs serving governmental constituents.

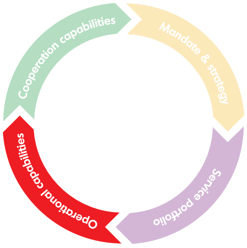
As CERTs regularly face challenges with data protection legislation when dealing with incidents, initiatives at the national and European level should be developed with the aim of **identifying best practices and developing templates to comply with data protection regulations**. N/g CERTs still have little authority to require telecom service providers and ISPs to implement security measures and changes. Because of this, n/g CERTs are advised to share best practices among themselves on how to collaborate with network operators and service providers in a way that can ensure a high level of compliance, while taking into consideration given limitations of authority.



Service Portfolio

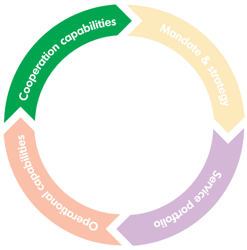
When exchanging information on incidents with their peers in other Member States, it is still common that partnering teams do not act upon information provided in a timely and professional way. For this reason, having a **standardised approach for information exchange** would be a useful contribution to mitigate the problem. A European forum like ENISA's working groups can be an appropriate venue for such discussions. Besides providing core services such as incident handling, n/g CERTs are encouraged to **bring in additional services and demonstrate added value to their constituents**, for example preparing national campaigns to raise awareness on cyber-security topics, organising national cyber-security exercises and involving relevant stakeholders. As the n/g CERTs are still not sufficiently involved in disaster recovery planning for critical information infrastructure, policymakers should support teams by giving them a stronger mandate. It is also important to increase transparency on the activities of n/g CERTs, for example by **making public the provision of statistics on incidents**.

1. Executive Summary



Operation

In order to alleviate the often quoted concern of limited funding for the activities of n/g CERTs, teams, if possible and within their mandate, should actively **look for alternative funding sources**. EU-financed projects and commercial & research projects are among the possible sources. As for their staffing policy, n/g CERTs need not only to attract highly specialised technical personnel but also **look for legal skills and**, last but not least, **PR (public relations) experts** to give more visibility to the activities of n/g CERTs. This relates, for example, to the provision of services on a 24/7 basis, which is still not sufficiently communicated to stakeholders in the area of cyber-security. Owing to the fact that highly specialised training for staff is expensive, the n/g CERTs across the region (potentially aided by ENISA) should look for efficiencies, offering **mutual assistance when participating in specialised courses** as well as identifying topics of interest to them to be covered in ENISA's workshops and other CERT associations' initiatives.



Cooperation

Even though a very good level of cooperation within international forums is an obvious benefit and indispensable need for the n/g CERTs in many aspects of their work, **national and regional cooperation should be promoted more actively and explored by the teams**. There is still room to improve the level of cooperation between n/g CERTs and domestic stakeholders in the area of cyber-security by engaging in local working groups and informal meetings, as well as drawing up voluntary written agreements. To overcome or partly solve the current challenge posed by legal obstacles when collaborating and sharing information on cyber-security incidents, bilateral or multilateral agreements should be considered by teams with regard to different partners such as ISPs, private sector companies like banks, and law enforcement authorities (LEAs). A key **focus should be maintained with law enforcement aspects of cybercrime** to increase the quality of cooperation between n/g CERTs and LEAs, which in some cases can be one-sided as LEAs are not always willing or allowed to share information regarding criminal investigations. Best practices that have been developed by CERT initiatives and forums need to be followed by the individual teams in their interactions with LEAs.

Despite clear progress in implementing baseline capabilities, n/g CERTs still face a number of obstacles mainly (but not exclusively) of a political, legal and financial nature. Therefore it is necessary that measures are taken by stakeholders domestically as well as on a European level to mitigate these obstacles.

2

Introduction

2 Introduction

2.1 General Context

The n/g CERTs[3] play a key role in protecting the critical information infrastructure (CII) that forms a vital part of a nation's economy and society. In the complex environment of cyber-security they are instrumental in coordinating incident management with the relevant stakeholders at the national level. They also bear responsibility for cooperating with national/governmental teams in other countries on incident response. This capability is critical as the Internet does not stop at national borders, which makes it necessary to enhance cooperation among n/g CERTs with regard to information sharing and coordinated incident response.

[3] The term national/governmental CERT was introduced to cover the different types of national, de facto national and governmental CERTs. The n/g CERTs are in charge of: a) generally supporting the management of security incidents for systems and networks within their country's borders; b) bearing responsibilities for the protection of critical information infrastructure (CIIP) in their country; c) acting as official national point of contact for n/g CERTs in other Member States. For definitions of the terms 'national', 'governmental', 'national/governmental' and 'de facto national' CERT see glossary (Annex 1). Note that definitions may vary across Member States.

2.1 General Context

On a European level, the importance of CII and the role of n/g CERTs in protecting it have been stressed on numerous occasions in various strategy and policy documents.

In its **Communication on Critical Information Infrastructure Protection (CIIP)**,[4] the European Commission highlights the importance of national/governmental CERTs:

> *A strong European early warning and incident response capability has to rely on well-functioning National/Governmental Computer Emergency Response Teams (CERTs), i.e. having a common baseline in terms of capabilities.*

In its **Communication 'A Digital Agenda for Europe'**,[5] the European Commission affirms the role of national/governmental CERTs as a key player in the area of trust and security:

> *[...] to react in real-time conditions, a well-functioning and wider network of Computer Emergency Response Teams (CERTsshould be established in Europe by 2012.*

In order for n/g CERTs to carry out properly their roles described above it is important that the Member States equip them with sufficient capabilities in the following categories:

- **Mandate & strategy** relates to the powers and justification in a form of a strategic document on cyber-security that need to be granted to the team by the respective government;
- **Service portfolio** covers the services that a team provides to its constituency or is using for its own internal functioning;
- **Operational capabilities** concern technical and operational requirements a team must comply with; and
- **Cooperation capabilities** encompass requirements regarding information sharing with other teams that are not covered by the previous three categories. They also refer to cooperation with all other stakeholders in the area of cyber-security such as policymakers, the military, regulators, (critical information infrastructure) operators, law enforcement authorities, etc.

[4] 'Protecting Europe from Large Scale Cyber-attacks and Disruptions: Enhancing Preparedness, Security and Resilience' (COM(2009) 149): http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

[5] 'A Digital Agenda for Europe' (COM(2010) 245): http://ec.europa.eu/information_society/digital-agenda/index_en.htm

2.2 Rationale

The aim of this report is to deliver an updated set of ENISA's recommendations on baseline capabilities for n/g CERTs in Europe. In 2009 and 2010 ENISA carried out its very first attempt to define a minimum set of baseline capabilities[6] that a CERT in charge of CIIP in Member States should possess to take part and contribute to sustainable cross-border information sharing and cooperation. At the same time, defining capabilities is an ongoing process which has to reflect changes in the cyber-security environment and technological development in general. Although many Member States have established their n/g CERTs since ENISA published its first recommendations in 2009/2010, the capabilities of these teams can vary substantially across Member States.

For these reasons, ENISA has launched a project with the aim of reviewing the existing recommendations of baseline capabilities, assessing their adequacy for the current environment as well as the level of deployment in the Member States. This report focuses on the updating and addition of recommendations on baseline capabilities for n/g CERTs while using the inputs of the accompanying report 'Deployment of Baseline Capabilities of National/governmental CERTs – Status Report 2012'.

[6] http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities

2.2 Rationale

2.2.1 Background information and motivation

With respect to the 'Digital Agenda for Europe' communication mentioned earlier, which calls for the establishment of a well-functioning network of CERTs at the national level covering all of Europe, ENISA assessed this topic in its annual Work Programmes (WP).

In 2012 ENISA started a stock-taking project 'Further definition and deployment of baseline capabilities for national/governmental CERTs' with two principal objectives:

- to assess the level of compliance of n/g CERTs in EU Member States with currently defined baseline capabilities and to provide a status report on the level of deployment of the current set of baseline capabilities (the aim of the separate report 'Baseline Capabilities of National/governmental CERTs – Status Report 2012');
- to further discuss the baseline capabilities with CERTs, and where appropriate adjust and extend the currently defined baseline capabilities with a focus on national and regional cooperation (the aim of this report).

The overall aim of the project is to provide Member States with a common denominator to follow with regard to the capabilities of n/g CERTs so that the outstanding gaps in cooperation are closed as far as possible.

The original Baseline Capabilities document consists of two parts. Part I was published in 2009 and included concise recommendations on baseline capabilities, focusing on operational/technical matters. It was very well received by the CERT community. In 2010 ENISA published Part II of the document, which made further improvements and presented a comprehensive set of policy recommendations regarding baseline capabilities of n/g CERTs.

In this report on an updated set of baseline capabilities recommendations (now merged into one document), as well as in the accompanying report 'Deployment of Baseline Capabilities of National/governmental CERTs – Status Report 2012', the structured approach of the original ENISA document is followed. This means that capabilities are categorised according to four areas:

- Mandate & Strategy;
- Service Portfolio;
- Operation;
- Cooperation.

Mandate & strategy
Service portfolio
Operational capabilities
Cooperation capabilities

Recommendations in this report focus primarily on how to address the gaps identified in 'Deployment of Baseline Capabilities of National/governmental CERTs – Status Report 2012'. As a reference, the full list of original recommendations from the 'Baseline Capabilities of National/Governmental CERTs Policy Recommendations' published in 2010 is included in Annex VII: List of original policy recommendations on Baseline Capabilities.

2.2 Rationale

2.2.2 Target audience

The intended target audience for this report (apart from n/g CERTs) primarily consists of ENISA, policymaking bodies at national and EU level with responsibility for establishing and operating n/g CERTs, service providers, network operators, other private sector companies, law enforcement authorities and others.

2.2.3 Previous projects or work

ENISA is carrying out comprehensive surveys of and producing reports on various aspects of the operation of n/g CERTs with a focus on identifying best practices that these teams can follow and on enhancing their cooperation.[7] Some of the latest reports have been drawn upon in compiling this report. Apart from the original Baseline Capabilities document these included, for example, the following:

- *A flair for sharing – encouraging information exchange between CERTs (December 2011)*[8]

This study focuses on the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe.

- *CERTs Operational Gaps and Overlaps (December 2011)*[9]

This document analyses operational gaps and overlaps of national/governmental CERTs and provides some recommendations. Recommendations made in this report represent the results of analysis of input gathered from the relevant external stakeholders (European CERTs) and give additional ideas for ENISA experts to consider when planning future ENISA activities.

- *Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime – A first collection of practices (February 2012)*[10]

The essential aim of this report is to improve the capability of CERTs, with a focus on n/g CERTs, and to address the network and information security (NIS) aspects of cybercrime. The report focuses in particular on supporting n/g CERTs and their hosting organisations in the EU Member States in their collaboration with LEAs. It also intends to be a first collection of practices collected from mature CERTs in Europe.

All of these reports (along with others mentioned in section 3.1 on desk research) provided valuable insights and enriched findings for all four categories of capabilities.

[7] These activities are further supported by other initiatives, including organising (since 2005) annual workshops for national/governmental CERTs, whereby a general theme is set for each of these workshops. Recent workshops have focused on more technical 'deep dives' into topics like botnets and hands-on technical training.

[8] http://www.enisa.europa.eu/activities/cert/support/legal-information-sharing

[9] http://www.enisa.europa.eu/activities/cert/other-work/files/operational-gaps-overlaps

[10] http://www.enisa.europa.eu/activities/cert/support/supporting-fight-against-cybercrime

3

Methodology

3 Methodology

The following sources were used in completing this report: desk research based mainly on publicly available information, questionnaires distributed among the CERT community and other stakeholders involved in the area of CIIP, interviews held with several n/g CERTs and additional discussions at the annual FIRST conference in Malta in 2012,[11] as well as contributions of experts from the informal expert group. Further details on these sources are given below.

[11] http://www.first.org/conference

3.1 Desk Research

The project team relied mostly on secondary sources to gather information for the project until the questionnaires started to be returned and interviews conducted. The project team first reviewed all of the websites of n/g CERTs in the EU and EFTA Member States to prepare the basis for the internal report on deployment. Many CERTs are publishing a good deal of information on their websites in English, including the RFC 2350[12] documents. Additionally, some information was generated by content from the websites of CERT associations and initiatives such as FIRST and Trusted Introducer and the websites of policymakers and other stakeholders in the area of cyber-security. Work carried out by ENISA regarding various aspects of the functioning of n/g CERTs was also an important source of information for the project (see Annex III). These ENISA reports were used in conjunction with reports that are still being drafted but which have some preliminary results shared. This contribution has proven to provide valuable synergies for this report. Last but not least, the project team also studied basic strategic documents and legislative tools on the European level pertaining to cyber-security. For a complete list of sources, see Annex III.

[12] http://www.ietf.org/rfc/rfc2350.txt

3.2 Survey

To gather the views of stakeholders on the baseline capabilities of n/g CERTs, an extensive survey was designed that covered all four categories of baseline capabilities and the respective recommendations. Respondents to the questionnaire were also encouraged to provide additional feedback. Two versions of the questionnaire were distributed, one for n/g CERTs (the actual focus of the reports) and the other for other stakeholders (all other CERTs, regulators, policymakers, ISPs and telecommunication operators or vendors). The reason for a more extensive questionnaire was the intention to provide stakeholders' input for two reports – this report on updated baseline capabilities, and the accompanying report 'Baseline Capabilities of National/governmental CERTs – Status Report 2012'. The full versions of the questionnaire are attached to this report in Annex IV: Questionnaire for national/governmental CERTs and Annex V: Questionnaire for other stakeholders (other than national/governmental CERTs).

While the aim of the questionnaire for n/g CERTs was to allow these teams to assess how they function, the questionnaire for the other stakeholders aimed to provide the outside view of constituents which are recipients of services provided by n/g CERTs. This approach was useful for balancing opinions of the n/g CERTs with the opinions of their constituents and thus delivering the whole picture on the activities of n/g CERTs in EU Member States.

In total, more than 240 respondents[13] were contacted regarding the survey and most of them received the questionnaire by email. The survey covered all 27 Member States of the EU plus three countries of the European Free Trade Association (EFTA) – Iceland, Norway and Switzerland. All national/governmental and other CERTs from the ENISA CERT Inventory[14] received the introductory letter and the questionnaire.

[13] This number is cleared from invalid or double contacts, because in some cases the contacted person was no longer working in the organisation contacted, the organisation no longer existed or was merged with or transformed into other organisation etc.

[14] http://www.enisa.europa.eu/activities/cert/background/inv

3.2 Survey

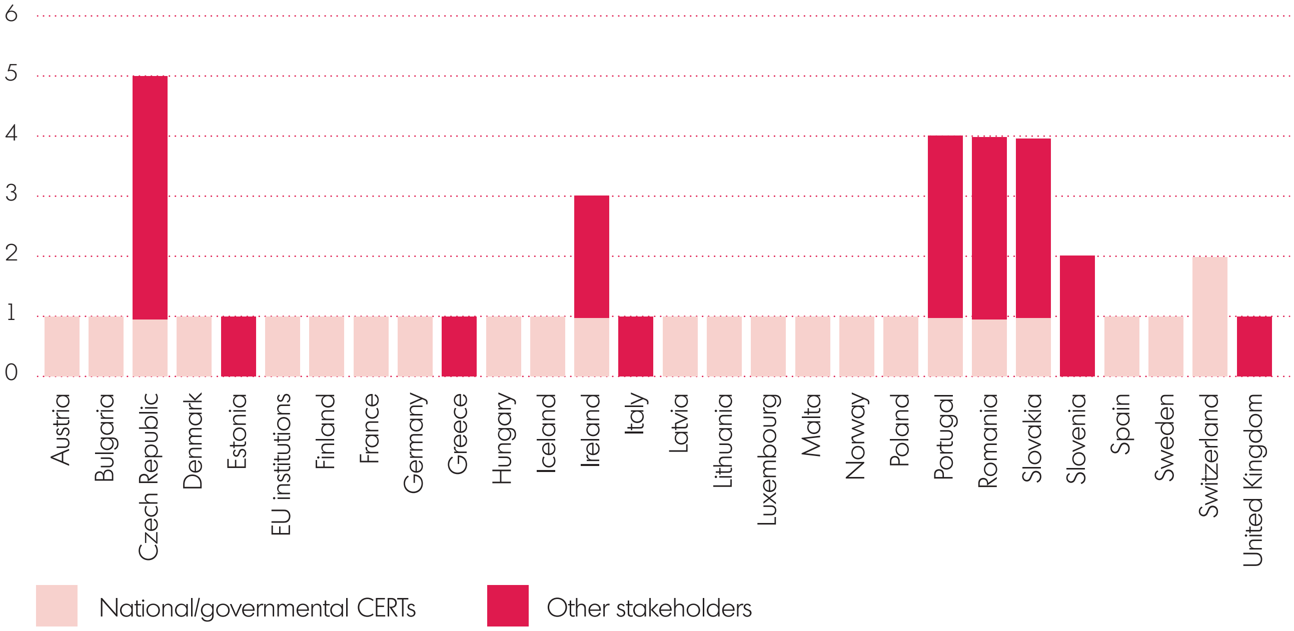
The survey was distributed to other stakeholders such as policymakers, regulators, operators, vendors and others, using ENISA's email lists and/or the contractor's own contacts.

The distribution of questionnaires started in May 2012 and a series of email reminders followed to speed up the process of replies. The email reminders were in many cases accompanied by phone calls in order to achieve a high response rate. The final total number of returned questionnaires by the beginning of August reached 45, of which 25 were from n/g CERTs including the CERT for EU institutions (CERT-EU) and 20 were from other CERTs and other stakeholders. In total, respondents from 27 countries (including three EFTA countries) returned the questionnaire, which provided a highly representative sample for analysis. In the case of three EU countries there was no response from either n/g CERTs or other stakeholders.

For details on the survey respondents according the type of organisation and country of origin see Figure 1.[15]

Figure 1:

Survey respondents by country and type of organisation



n=45 (25 n/g CERTs plus 20 other stakeholders)

[15] Please note that three responding CERTs in Romania identified themselves as being either national or governmental, although they are not listed as such in relevant databases of ENISA (http://www.enisa.europa.eu/activities/cert/background/inv) or Trusted Introducer (https://www.trusted-introducer.org/teams/country_LICSA.html). Also in the case of the Czech Republic, a state agency claimed to be a governmental CERT, although at the time of writing the report, the respective n/g CERT still had not been established. The category of other stakeholders refer to all other CERTs, policymakers, regulators and other government agencies as well as operators and service providers.

3.3 Interviews

The project team used the information gathered from stakeholder surveys and approached selected stakeholders with a request for additional input through interviews. This approach has proven to be beneficial in many of the previous projects carried out by ENISA. The interviews concerned topics that were not included in the already extensive questionnaire (see Annex VI: Discussion Guide for Interviews), but also served to clarify answers given in the survey. In addition, the interviews provided a chance for the stakeholders to offer a free flow of thoughts beyond the original discussion guide.

In total, the contractor carried out eight interviews with n/g CERTs from EU Member States in July and August 2012. Interviews were conducted by telephone (in English and in one case also in the local language of the interviewee), with one exception, when the respondent preferred to answer additional questions by email. The interviews lasted about one hour on average . It turned out to be helpful that the contractor sent a brief interview guide ahead of the interviews, which allowed the interviewees to be better prepared, including provision of additional written materials.

3.3.1 Discussions carried out during the FIRST 2012 Conference

From 17–22 June 2012, the annual conference of the FIRST forum[16] took place in Malta.[17] A project team member, who also took part in the conference, established valuable contacts with a number of n/g CERTs and engaged in talks (not full-scale interviews due to the limited time available during conference sessions) with several n/g CERTs at the conference. The team member agreed with them that they would participate in the project by returning questionnaires and/or by phone interviews. The FIRST conference also provided full access to its documentation, including presentations by n/g CERTs. The evolving role of n/g CERTs was the primary focus of the policy and management section of the conference.

3.4 Informal Expert Group

An important input to this report was provided by a group of n/g CERTs, other CERTs, and other stakeholders who volunteered to take part in the Informal Expert Group. The aim of the Group was to review the two deliverables produced in the framework of the project – the report on deployment of current set of baseline capabilities for n/g CERTs and the updated set of these baseline capabilities using the input of stakeholders. All of the survey respondents were offered the opportunity to take part in this group at the beginning of the survey. In the end, 15 respondents agreed to send their feedback on the reports to the project team.

[16] http://www.first.org/

[17] The conference was preceded by an annual CERT workshop organised by ENISA at the same place, which focused on hands-on technical training for national/governmental CERTs (http://www.enisa.europa.eu/activities/cert/events/7th-cert-workshop).

4

Contents of this report

4 Contents of this report

In the following four chapters, new and updated recommendations for all baseline capabilities of n/g CERTs are presented. Consequently, the focus is shifted and the goal is to address only those attributes of capabilities where gaps still exist or have been newly identified.

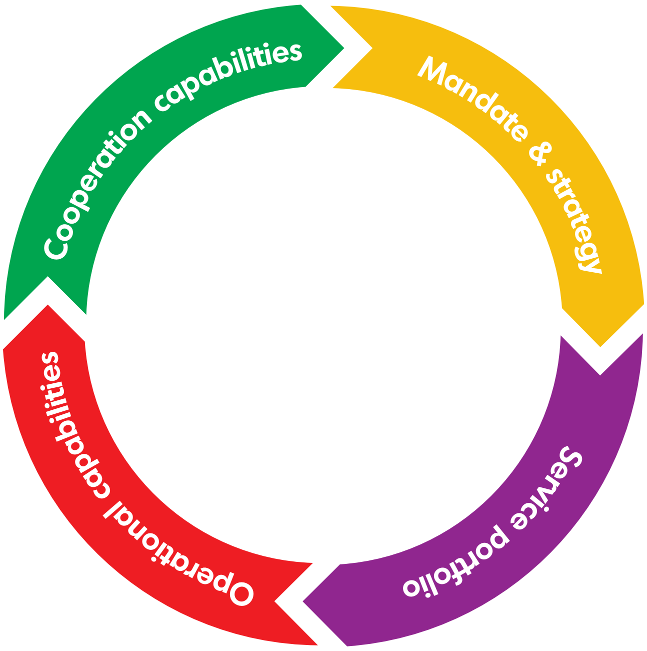
The recommendations follow a similar structure to the accompanying report, 'Baseline Capabilities of National/governmental CERTs – Status Report 2012'.

Each of the gaps identified in the previous study are listed in this report, along with the recommended approach to resolving the shortcoming. These recommendations are either new ones relating to issues that have come up in this year's research, or updates of old recommendations where the level of compliance is still not considered satisfactory.

The aspect of regional and national cooperation was considered. At the same time, the recommendations are targeted to various stakeholders in the area of cyber-security, including n/g CERTs, policymakers, CII operators and others. Also, comments are attached as to the time character (short-, medium- or long-term approaches) of the recommendations and possible barriers to their implementation.

For reference purposes, the policy recommendations published in 2010 are included in Annex VII: List of original policy recommendations on Baseline Capabilities.

An overview of the four chapters on n/g CERT capabilities is listed below, illustrating how each chapter is structured according to relevant topics. Each chapter introduces the capabilities, identifies a number of gaps and recommendations, and provides an overview of the current situation regarding the relevant n/g CERT capabilities supported by select indicators from ENISA's survey of n/g CERTs.



5. Mandate & Strategy

National Cyber-security & CIIP Strategies

- Gaps and Recommendations
- Situation Overview
  - CIIP Capabilities
  - Maturity of Cyber-security Strategy

Mandate

- Gaps and Recommendations
- Situation Overview
  - Hosting Organisation
  - Constituency
  - Roles and Responsibilities of n/g CERT

6. Service Portfolio

National/Governmental CERT Core Capabilities

- Gaps and Recommendations
- Situation Overview
  - Incident Handling
  - National PoC for Incident Reporting and Information Dissemination
  - CIIP

Proactive Services

- Gaps and Recommendations
- Situation Overview
  - Technology Watch, Announcements
  - Security and Vulnerability Assessment
  - Providing Guidelines on Security Configuration
  - IDS

Reactive Services

- Gaps and Recommendations
- Situation Overview
  - Incident Handling
  - Alerts and Warnings
  - Vulnerability Handling
  - Artifact Handling

Security Quality Management Services

- Gaps and Recommendations
- Situation Overview
  - Awareness Building
  - Education and Training
  - Business Continuity Management
  - Risk Management

7. Operation

Human resources

- Gaps and Recommendations
- Situation Overview
  - Team
  - Operation Mode

Infrastructure

- Gaps and Recommendations
- Situation Overview
  - Communication Services
  - Logical Security
  - Physical Security

Business Continuity

- Gaps and Recommendations
- Situation Overview
  - Ensuring Continuity

Provision of Services

- Gaps and Recommendations
- Situation Overview
  - Supporting Processes and Tools

8. Cooperation

National Cooperation

- Gaps and Recommendations
- Situation Overview
  - Constituency
  - ISPs and Other CII Providers
  - Law Enforcement

Cross-Border Cooperation

- Gaps and Recommendations
- Situation Overview
  - Initiatives in Cooperation

Best Practices for Cooperation

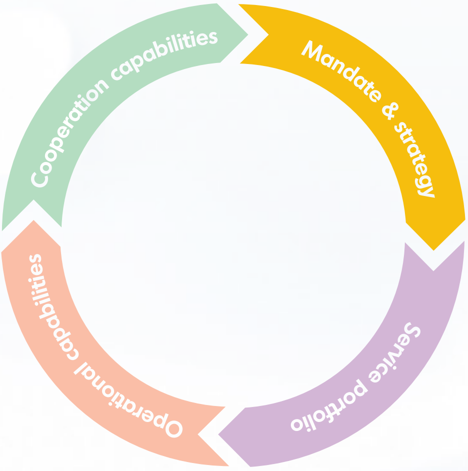
- Gaps and Recommendations
- Situation Overview
  - Quality of Information
  - Sustainable Reaction
  - Common Terminology and Schemes

5

Mandate & Strategy

5 Mandate & Strategy

Mandate & Strategy capability covers the powers and justification that need to be granted to the n/g CERT by respective governments. It also relates to the hosting organisations for the n/g CERTs and constituents to whom the n/g CERT provides its services. An overarching topic is the existence of national cyber-security strategies, in which the mission of the n/g CERT in the area of cyber-security should be embedded.



5.1 National Cyber-Security & CIIP Strategy

European policymakers have gained significant insights into how to protect their countries' critical information infrastructures from their experiences in establishing national and governmental CERTs. They understand that effective and coordinated approaches are needed to respond to cyber-incidents, threats, and attacks that can impact both the public and private sectors. As the EC has previously recognised, Member States' adoption of holistic approaches to cyber-security and the protection of critical information infrastructures is integral to developing a strong pan-European network and information security policy.

ENISA's original 'Policy Recommendations on Baseline Capabilities of National & Governmental CERTs', *published in 2010, recommended a number of key actions that policymakers in the Member States should take, including:*

- establishing and developing cyber-security as a part of national policy;
- identifying a leader in the overall national cyber-security effort as well as appropriate experts and policymakers within the public and private sectors, and establishing cooperative arrangements among stakeholders;
- identifying expert counterparts internationally and fostering initiatives in collaboration with these individuals and organisations;
- establishing an integrated risk management process for identifying and prioritising protective measures regarding cyber-security;
- assessing and periodically reassessing the current state of cyber-security efforts and the development of programme priorities.

EU Member States have taken steps to implement and improve their strategies covering CIIP and cyber-security in the last few years, but there remain opportunities for further development in this area.

5.1.1 Gaps and recommendations

There are already several national cyber-security strategies in place, which take a holistic approach to this topic. ENISA continues to encourage all Member States to draft such strategies.[18] N/g CERTs are also supported by ENISA in finding optimal ways to share data and act upon them without violating the sensitive issue of data protection rules.[19]

[18] ENISA's Good Practice Guide on National Cyber Security Strategies: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss

[19] A study carried out by ENISA, 'A flair for sharing – encouraging information exchange between CERTs': http://www.enisa.europa.eu/activities/cert/support/legal-information-sharing

5.1 National Cyber-Security & CIIP Strategy

Gap:

National cyber-security strategies are still often not in place, and where they are, in some cases the role of the n/g CERT is not mentioned and/or specified.

Recommendations:

These are short-term to medium-term recommendations. There may be some political obstacles including changes of government, which might slow down the process of drafting the national cyber-security strategies.

- Member State policymakers should ensure that formalised national cyber-security strategies are put in place as soon as possible and **define as specifically as possible** the role of the n/g CERT in these strategies.
- Heads of n/g CERTs should use their status, influence, and hosting organisation's position within the government to ensure that their respective team(s) has a **defined, long-term position** in creating these strategies going forward.
- To the extent that an n/g CERT is finding it challenging to establish a role in developing the national cyber-security strategy, then the n/g CERT should try to cooperate with other interested stakeholders, including critical information infrastructure providers, other CERTs, and law enforcement agencies, to raise awareness of the **importance of including the CERTs in developing cyber-security strategies**.
- ENISA needs to distribute to relevant stakeholders the results of its research on implementation of national cyber-security strategies in the Member States. Results from this study should be used by stakeholders across the region to **draw on best practices for formalising their national cyber-security strategies** and ensuring that they have a role in developing these strategies.

Gap:

N/g CERTs continue to face problems with data protection legislation.

Recommendations:

These are rather long-term recommendations, which require not only revising the legislation (data protection legislation is currently being drawn up on the EU level), but also influencing the data protection authorities.

- Member State policymakers and heads of n/g CERTs need to take steps to ensure that n/g CERTs can both carry out their mandate and **adhere to national and EU data protection legislation.**
- N/g CERTs – especially team leaders and legal specialists – should put in place procedures and **best practices that require their staff to handle data in compliance with EU rules** and their Member State's laws. The risks to an n/g CERT's reputation from a data breach or misuse of personal data are too significant for an n/g CERT to risk non-compliance with data protection legislation.
- Consideration should be given to establishing working groups at international or regional meetings – including ENISA meetings – at which n/g CERTs discuss best practices and the potential **for instituting common data handling protocols.** This would provide a basis from which n/g CERTs can operate with confidence that they are upholding data protection legislation and principles.
- At national level, the n/g CERTs might consider establishing thematic working groups on data protection to involve interested stakeholders such as the banking industry, and to improve overall information exchange.
- N/g CERTs need to **consider hiring or engaging a legal expert specialising in IT security issues** in order to avoid uncertainty regarding the handling of personal data. It should be acknowledged, however, that this could be a costly option.

5.1.2 Situation overview

CIIP capabilities

Having full national CIIP capabilities requires Member States to take a number of steps, including: establishing a mandated (governmental) actor for strategic leadership and governance (such as a ministry or other policymaking body); having a coordination centre for cyber-security; and having a centre for technical expertise (CERT). Each of these entities should then interact with relevant stakeholders in that country. The role of the n/g CERT within this strategy is to prevent, detect, deter, respond to, and recover from cyber-incidents.

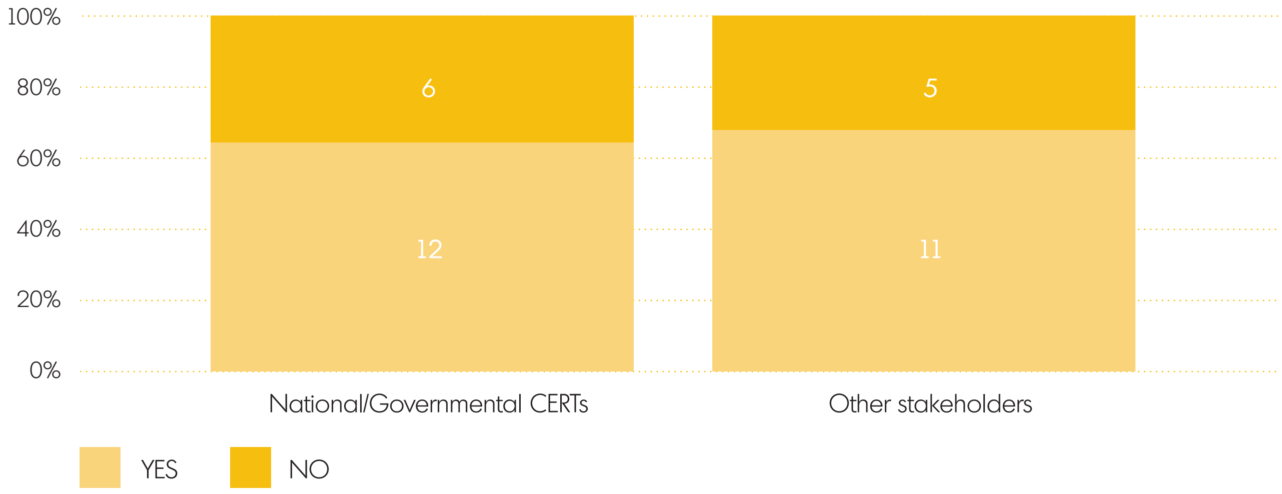
5.1 National Cyber-Security & CIIP Strategy

Maturity of cyber-security strategies

Feedback from Member State n/g CERTs suggests that there is increasing harmonisation in terms of the roles, responsibilities and capabilities of n/g CERTs, but there remain fundamental differences between EU Member States in terms of the maturity of their national cyber-security and CIIP strategies and the roles that their n/g CERTs play. For example, there are some n/g CERTs that are hosted by non-governmental organisations and not all n/g CERTs have a formal mandate. Further, not all n/g CERTs believe that their mandate clearly sets out their roles; only slightly over 60% of n/g CERTs (and nearly the same percentage of respondents among other stakeholders) reported that their mandate is clear with regard to the basic services that they provide (see Figure 2).

These differences reflect the continued challenges that Member States face in implementing cyber-security strategies that have similar structures and to promote cooperation across many countries with different resources and strategies.

Figure 2:
Opinions on the clarity of the mandate of n/g CERTs



N (number of respondents) =34 (18 n/g CERTs + 16 other stakeholders)

Now, Member States are taking steps to update their approaches to cyber-security and CIIP through new legislation. Slightly fewer than half of n/g CERTs report that their governments are drafting or considering legislation that impacts cyber-security, and have generally sought input from the country's n/g CERT on such legislation.

In terms of being involved in the development of national cyber-security strategies, almost all Member States' n/g CERTs report that they either serve on bodies that develop national cyber-security laws/ strategies or advise these bodies informally. Further, many n/g CERTs reported that they are involved in the risk management process regarding national critical information infrastructure protection, whether formally or informally. A number of respondents said that they are pleased with their government's cyber-security approach, but several noted that more could be done to ensure cooperation at the domestic level.

5.2 Mandate

An n/g CERT should play a key role in a Member State's overall national strategy for cyber-security alongside other important players and stakeholders, such as: policymakers, national regulatory authorities, industry associations (e.g., telecoms, banking and energy), law enforcement agencies, and other industry CERTs. Within the national strategy, an n/g CERT should be mandated with and given a specific set of roles and responsibilities and an official framework to guide its actions. As discussed in section 5.1, not all Member States have provided their n/g CERTs with a formal mandate, which is a critical first step in enabling these CERTs to accomplish their objectives. The mandate needs to be clear enough to define the roles and powers of n/g CERTs in the national cyber-security environment.

5.2.1 Gaps and recommendations

There has been significant progress in recent years regarding the establishment of n/g CERTs across Europe and giving them legal footage to fulfil their tasks. It is now important that the mandate is made clear to avoid uncertainty among the constituents of n/g CERTs as well as among other stakeholders in cyber-security. The need for clarity pertains, for example, to the powers of n/g CERTs to be able to solve certain kinds of incidents without involving LEAs.

Gap:

The mandate, especially the definition of roles and responsibilities, needs to be clear enough to support all relevant activities of the n/g CERT.

Recommendations:

These are recommendations of an ongoing character, which aim to respond to current trends in cyber-security necessitating changes in the mandate of n/g CERTs.

- Member State policymakers should cooperate with the heads of their n/g CERT(s) to ensure that the team's mandate lays out its role and responsibilities clearly and concisely, including the governmental CERT function. It is very important to **eliminate the duplicate tasks and activities when there are several n/g CERTs in a country.**
- The n/g CERT's head must communicate a clear understanding of its mandate to his/her team to ensure that the team carries out the mandate.
- The n/g CERT's head also has responsibility in the longer term to work with policymakers and his/her hosting organisation to make sure that the team has the resources and staffing to carry out the mandate.
- N/g CERTs should ensure that there is ongoing discussion among various key staff members – including incident handlers and technical experts – and with key constituents such as the government bodies and critical information infrastructure bodies about whether **the mandate matches its actual role and responsibilities and whether the mandate meets the needs of these constituents**.
- Before the mandate is specified/clarified by the government, the n/g CERTs need to look for neighbouring or other n/g CERTs for inspiration and best practices on how to secure the operational capacities.

5.2 Mandate

Gap:

The mandate of n/g CERTs needs to be publicly announced.

Recommendations:

These are short-term recommendations, which may be impeded only if there are serious reasons not to publish the details of the mandate of the n/g CERT.

- Member State policymakers and n/g CERTs should agree on processes for **making the mandate available to the public** – unless there are compelling reasons not to do so.
- N/g CERTs across Europe should try to establish a common way of making the mandate available to the public, such as through a direct link on their homepage, potentially through the ENISA platform.
- **Informal** discussion between n/g CERTs regarding best practices for presenting the CERTs' mandate to the public can be carried out at ENISA conferences or through informal dialogue between these CERTs.

Gap:

Special provision including funding need to be included for the national and governmental CERT-type roles and functions.

Recommendations:

These are short-term to medium-term recommendations. The implementation of the recommendation will require provision of funding resources, which might be a challenge in the current economic environment in Europe.

- Member State policymakers and heads of n/g CERTs need to ensure that n/g CERTs with responsibility for the governmental networks have adequate funding and support for carrying out this important function in the long term.
- Policymakers and n/g CERTs should also try to include the n/g CERT's role and responsibilities in its mandate and include funding provisions in the mandate.
- Member State n/g CERTs should consider using the ENISA platform over the longer term to **develop a common vision for what types of support their governments should provide** for those serving in the governmental CERT capacity, especially regarding funding and cooperation with other domestic CERTs.
- Teams that provide the CERT services to the government on a temporary basis until the new n/g CERT is established, need to have **written agreements with the government,** which define the scope of services to be provided, funding for the services provided, and potentially allocation of resources and securing of seamless communication facilities.

Close collaboration between CERTs should be assured in those cases when the national and governmental functions are provided by different CERTs.

5.2.2 Situation overview

Hosting organisation

The legal framework in which an n/g CERT operates depends on matters such as its official mandate and its hosting organisation. The vast majority of n/g CERTs reported that they are hosted in or operated by a 'higher' organisation, although there is much variation in the types of organisation that host these CERTs. About three-fifths of n/g CERTs said that they are hosted by organisations responsible for the development of the country's national cyber-security agenda. Others, though, are hosted by organisations without responsibility for their country's cyber-security agenda, including private sector actors or university departments. Most n/g CERTs reported having a direct line of accountability to an appropriate section within the national executive in the event of an emergency, either on a formal or informal basis.

A number of Member States' n/g CERTs are hosted by 'national cyber-security centres', including the United Kingdom, the Netherlands, France and Ireland, and a similar arrangement is being considered in the Czech Republic as well. These types of centres act either as independent agencies or as part of hosting agencies, and have at least some responsibility for the country's national cyber-security strategy. These organisations can also be responsible for monitoring the implementation of the national cyber-security strategy.

National telecommunications regulatory authorities (NRA) are another logical hosting organisation for n/g CERTs, although not as many Member States use this option. When an n/g CERT is embedded within a telecommunications NRA, it can make use of the NRA's institutional knowledge and powers; for example, NRAs may have authority over telecommunications providers in crisis situations. FICORA (Finland) is directly hosted by the Finnish telecommunications NRA, while CERT Bulgaria and CERT.RO (Romania) are either hosted by organisations within their countries' NRAs or are coordinated by the NRAs.

5.2 Mandate

Member States also charge other governmental organisations with hosting their n/g CERTs, including other ministries, institutes, or even private sector actors. For example, the Danish GovCERT is hosted by the Danish Ministry of Defence, and NorCERT is a part of Norway's national security agency. The use of universities or private sector actors to host some n/g CERTs reflects the fact that CERTs were initially established to provide security incident management services for a particular private sector or academic constituency. In the EU, CERT.LV (Latvia) is hosted by the Institute of Mathematics and Computer Science, University of Latvia, while CERT.AT (Austria) and CSIRT.cz (Czech Republic) are initiatives of the national top-level domain registries, which are private sector actors.

An n/g CERT's hosting organisation influences its reporting lines. CERTs that are embedded in a hosting organisation often must pass through the hosting organisation's structure to reach the national executive if the hosting organisation is not already a part of the national executive. According to CERTs, many of them operate under guidelines that establish the direct lines of communication and action proceedings in the event of security incidents that generally, but not always, involve a line of reporting that goes through the hosting organisation. Several n/g CERTs report that formal structures are in place or are being considered to give them a direct link to engage the national executive in crisis situations. In total, about half of n/g CERTs say that they have a formal direct line of accountability within the national executive, another 40% say they have an informal line of accountability, and just 10% reported that they have no direct line of accountability at all.

CERT respondents reported that they generally function well within their hosting organisations. There were no reports of tension between CERTs and their hosting organisations, although there was some sentiment that lines of communication for CERTs could be improved so that n/g CERTs have more direct access to relevant stakeholders at the governmental levels. Survey results show that EU Member States use a number of different governmental and even private sector organisations to host their n/g CERTs; logically, these hosts have different institutional focal points and resources.

Constituency

A CERT's constituency refers to the customer base for its services. Therefore, an n/g CERT's constituency consists of all entities within the state's borders because any domestic entity is a potential customer. The constituency of an n/g CERT can generally be broken down into subgroups based on the services that the CERT provides to each group or the responsibilities that it has for each group. According to the original 'Policy Recommendations on Baseline Capabilities of National & Governmental CERTs', an n/g CERT's constituent subgroups include:

- Government and public bodies: An n/g CERT provides its full range of services to the governmental and public bodies in its state.
- Critical information infrastructure organisations: An n/g CERT may provide its full range of services to CII organisations, but these organisations will often have their own IT or information security personnel responsible for handling security incidents. When this is the case, an n/g CERT can play a coordinating or supporting role to the CII organisation's personnel and capabilities. Nonetheless, the n/g CERTs should have a clear cooperation framework in place with CII organisations, even if they use their own IT security personnel.
- Other stakeholders within the state's borders: As the CERT-of-last-resort and national point of contact for cyber-security incidents, an n/g CERT may provide its services to any other constituents, including end users, other domestic CERTs, or any other domestic stakeholder, or the broader public interest.

'De facto' n/g CERTs may be charged specifically with serving other groups of constituents as well; for example, a research/education network CERT will likely also serve research and education networks, while a CERT created by a national domain operator will serve it.

The role of n/g CERTs as their country's CERT-of-last-resort means that they will always play a gatekeeping role that requires them to analyse incident reports to determine whether they arise from their constituents. If they do not, then the n/g CERT should forward the incident report to the appropriate body. In the event that the incident involves a government or public body, or is a CII organisation, or is not part of another CERT's constituency, then the n/g CERT will handle the incident report. Resource limitations mean that most Member State n/g CERTs will try to limit the extent to which they provide services to some constituency subgroups. Generally, their full services will only be offered to certain constituents such as the government, public bodies, and CII organisations. Beyond this, n/g CERTs can provide services to other constituents on a case-by-case basis.

N/g CERTs are somewhat uncertain about the breadth of their mandate, which can make it challenging for them to determine what activities fall within the mandate. This could mean that some CERTs are providing services to constituents that fall outside of their mandate, which may be counterproductive if resources are limited.

Roles and responsibilities for the n/g CERT

According to the original 'Policy Recommendations on Baseline Capabilities of National & Governmental CERTs', an n/g CERT should undertake a number of roles and responsibilities in its country, including:

- supporting the management of security incidents for systems and networks within its state's borders;
- contributing to the protection of critical information infrastructure within the state in the context of wider CIIP arrangements; and
- acting as the official national point of contact (PoC) for n/g CERTs in other Member States and worldwide.

5.2 Mandate

The original 'Policy Recommendations on Baseline Capabilities of National & Governmental CERTs' noted the importance for n/g CERTs of having an official government mandate to represent the country in international CERT communities, including FIRST (Forum of Incident Response and Security Teams) and potentially EGC (European Government CERTs). This mandate should include provisions for the CERT to act as the official national PoC for CERTs and other members of the security community in other countries. Having an n/g CERT that is clearly identified as a country's official PoC is an indispensable element of a national CIIP plan and is necessary for clear and flexible international collaboration between CERTs.

All n/g CERTs from Member States reported that they are an official PoC for other CERTs either formally or informally. Seventy percent of n/g CERTs reported that they have been formally given this designation, while the remaining 30% say that their designation is informal in nature. CERTs reported that having this PoC designation works well in terms of day-to-day operations with other countries' CERTs. Interestingly, several CERTs said that being their country's official PoC sometimes creates confusion at the national level about roles and responsibilities.

Serving as the national PoC for international CERT communities includes the responsibility for acting as a CERT-of-last-resort in situations of doubt or emergency. In addition, it means that n/g CERTs must often relay incident reports and other security-related information to the appropriate bodies in their country. It also means that, if no other appropriate entity can deal with a cyber-security incident, the n/g CERT may have to handle the incident.

It is also important that n/g CERTs exercise an active role in developing holistic national cyber-security and CIIP strategies. N/g CERTs should bear responsibilities for or play a role in CIIP planning (i.e. defining the scope of CIIP, identification of CII, and assessment of risks). Given that the n/g CERT will likely receive reports about significant security incidents, it makes sense for CERTs to be part of the national CIIP plan.

Thus far, Member State n/g CERTs do not yet uniformly participate in these processes. Just over half of n/g CERTs reported that their team is involved in their country's risk management process regarding the national CII, and several of these CERTs said that their activity is informal or ad hoc in nature. The fact that some n/g CERTs have not been in existence long could be one reason that they are not yet involved in these processes. Alternatively, some CERTs' governments may already look to other governmental organisations for support in implementing and monitoring the national CIIP strategy.

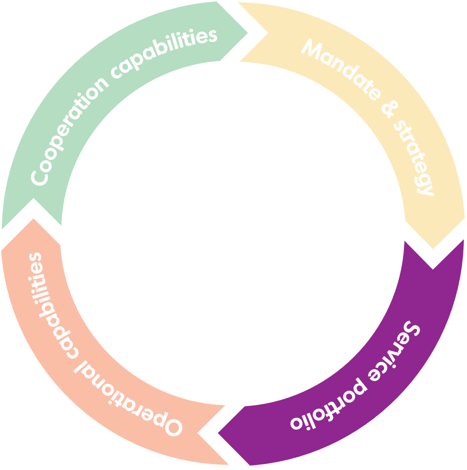
There are other roles and responsibilities that n/g CERTs can take on for certain constituents. For example, they could provide their expertise regarding cyber-security to other public and private institutions and organisations in their country, most importantly to LEAs. They could also work to organise, participate in, and promote sectoral or topic-specific initiatives in collaboration with other CERTs in their country or even international CERTs. The extent to which n/g CERTs provide these types of services depends on their mandate and resources.

6

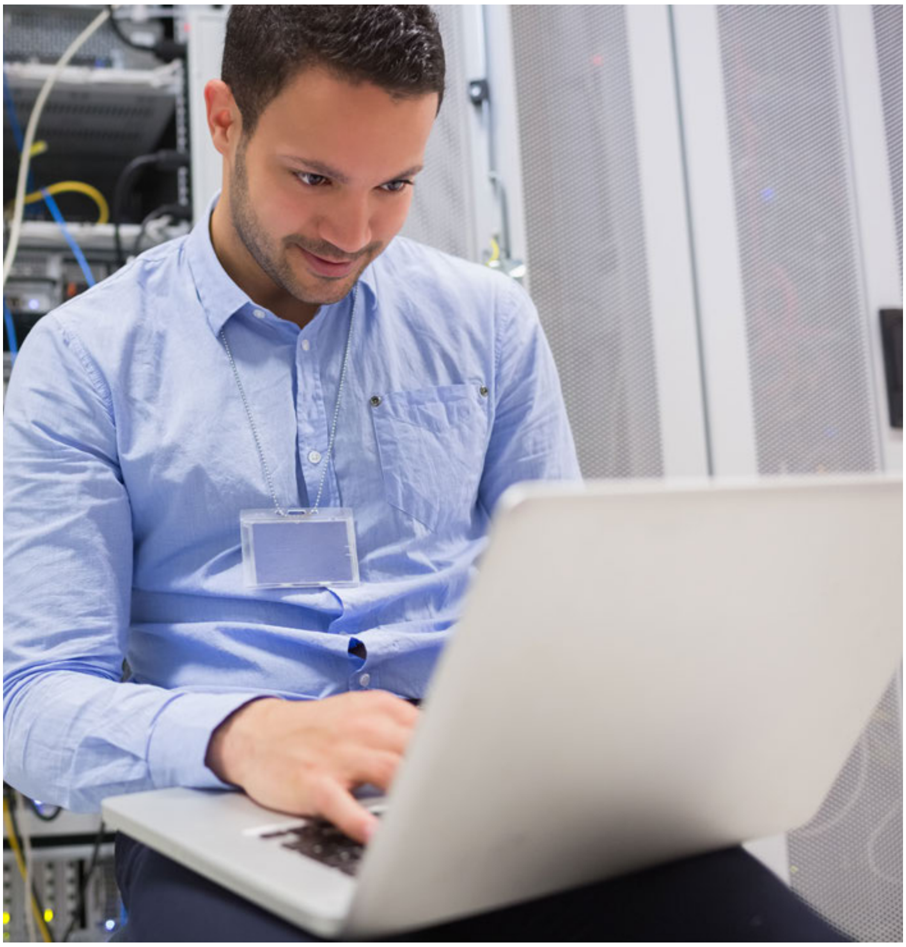
Service Portfolio

6 Service Portfolio

6.1 National/governmental CERT Core Services Capabilities



The service portfolio covers the services that an n/g CERT team provides to its constituency or is using for its own internal functioning. There are a number of core services that an n/g CERT is required to offer, but n/g CERTs can be flexible in offering additional services to support their constituents.



6.1 National/governmental CERT Core Services Capabilities

The service portfolio of an n/g CERT consists of the external services it provides to its constituency and its internal support processes. The original 'Policy Recommendations on Baseline Capabilities of National & Governmental CERTs' divides the external services that n/g CERTs commonly provide into three service classes:

- *Proactive services*, which are aimed at improving the infrastructure and security processes of a CERT's constituents before any incident or event occurs or is detected. By providing proactive services, CERTs help to avoid incidents and minimise their impact and scope when they do occur.
- *Reactive services*, which are aimed at responding to requests for assistance from a CERT's constituency, reports of incidents, and tackling threats made or attacks against the CERT's systems.
- *Other security quality management services*, which consist of services that improve an organisation's overall security. An n/g CERT should provide these services by leveraging its experiences from providing proactive and reactive services to its constituency and applying these experiences to quality management services.

Significant progress has been made in providing required services. Nonetheless, a number of issues should be addressed in order to ensure n/g CERTs can provide services according to their full potential.

6.1.1 Gaps and recommendations

To provide the services discussed above, an n/g CERT must also have appropriate internal support processes such as resource or infrastructure management processes. These supporting processes require adequate financial and personnel support as they are important to the continuing maturation of an n/g CERT.

Gap:

When handling incidents internationally, partnering n/g CERTs sometimes do not act as expected upon information provided. There can be a number of reasons for this. In some cases, this could be due to the lack of a standardised framework for the information that is exchanged, which makes it difficult for n/g CERTs to analyse and identify relevant information. But there are other factors. In some cases there can be legal/data protection barriers. In other cases, the mandate may not be sufficient.

Recommendations:

These are medium-term recommendations. There should not be significant obstacles to implementing the recommendations once a common approach is agreed, as most n/g CERTs are in favour.

- Heads of n/g CERTs should be proactive in discussing best practices regarding the use of information that is shared between n/g CERTs with their counterparts at other countries' n/g CERTs.
- Heads of Member States' n/g CERTs should create procedures and a culture at their n/g CERT that values and lays out the steps for considering and acting on information provided by other CERTs.
- In the longer term, n/g CERTs can pursue the creation of common norms regarding the handling of shared information through informal channels and discussions with other n/g CERTs, even if a fully standardised format for exchanging information between n/g CERTs is unlikely in the medium term.
- ENISA, FIRST or other CERT initiatives should serve as a platform for discussion of this topic. This discussion might result in a new study carried out by ENISA.

- Members of n/g CERT teams should be tasked with raising this issue at international meetings and forums with the aim of identifying key barriers to the efficient use and exchange of information. By identifying more specific causes, such as legal/data protection issues or clarifications that may be needed in the mandate, they could better act to address as many barriers as possible, and in the process aim to ensure a more efficient use of the information available.

6.1.2 Situation overview

The original 'Policy Recommendations on Baseline Capabilities of National & Governmental CERTs' *report points to core service capabilities that* n/g CERTs should have that are considered the most critical to their operation. These include:

Incident handling

Cyber-security incidents will inevitably occur, and it is vital that attacks and intrusions on national critical information infrastructure do not cripple the state for the duration of an attack. N/g CERTs must prioritise handling cyber-security incidents and incidents related to critical information infrastructure on a national and international scale. Such incidents can threaten a Member State's society (through economic, governmental, infrastructural, or ecological threats) and its population (e.g., incident at a nuclear power plant). Thus, responding to these incidents should take precedence over all other activities, and n/g CERTs need to be capable of responding as necessary to quickly contain and mitigate the incidents when they do occur.

Member State n/g CERTs reported that they provide incident handling services to at least certain constituents. Most n/g CERTs provide these services to their governments and other public bodies, and a number of them also provide these services to domestic critical information infrastructure organisations and even to other domestic CERTs. This reflects a baseline understanding – regardless of their mandate and other roles and responsibilities – that n/g CERTs have a central role in responding to cyber-attacks and intrusions on their country's critical information infrastructure.

National Point of Contact for incident reporting and information dissemination

Another central role for n/g CERTs is to serve as the national point of contact (PoC) for operational (24/7) incident reporting and as a disseminator of security-related information. Member States should provide their n/g CERTs with official PoC status in their mandate. Clearly stating PoC status facilitates clear and flexible national and international collaboration.

It is important for n/g CERTs to act officially as PoC for several reasons. First, foreign CERT teams must know who they should contact in a Member State regarding the sharing of security-related information and the reporting of incidents. Second, an n/g CERT is often best positioned of all potential organisations (including other CERTs and governmental organisations) to further disseminate information to other domestic CERTs and information security communities. Finally, having an official PoC status allows an n/g CERT to represent its country in international CERT communities.

Seventy percent of CERTs reported that they have formal status as their country's official PoC for cyber-security-related incidents and dissemination of information, with the other 30% saying that they have this status on an informal or *de facto* basis. CERTs report that cooperation based on their PoC status on the international level has been strong, but several CERTs reported that their PoC role has created some confusion on national level. Cooperation between n/g CERTs and other government actors will become even more important as n/g CERTs mature and fulfil a broader mandate, so all interested governments and organisations should strive to facilitate cooperation between n/g CERTs and other governmental organisations by clarifying their POC status and a mandate to the extent possible.

Critical Information Infrastructure Protection (CIIP)

N/g CERTs do not have fixed roles in terms of providing protection for national critical information infrastructures. CERTs are capable of providing a number of services in addition to their incident handling services. Examples of such services include risk analysis, security consulting, security assessment, and intrusion detection services. The exact role that an n/g CERT plays will depend on the national strategy for CIIP and the n/g CERT's mandate and defined responsibilities.

In the context of critical information infrastructure protection, the original 'Policy Recommendations on Baseline Capabilities of National & Governmental CERTs' *recommended that* n/g CERTs provide services in addition to those listed above, such as:

- announcements informing constituents about new developments that will have an impact on cyber-security in the medium- to long term, such as newly discovered vulnerabilities;
- security-related information sharing that provides their constituents with a comprehensive and easy-to-find collection of useful information and guidelines for improving security;
- alerts and warnings disseminating information that describes intruder attacks, security vulnerability, intrusion alerts, computer viruses or hoaxes, etc., and provide a short-term recommended course of action for dealing with these problems;
- awareness-building that provides information and guidance for organisations to better conform to accepted security practices and organisational security policies.

These services deliver additional value to a CERT's constituency in an efficient manner, as most n/g CERTs can provide such services to broader ranks of their constituencies at minimal cost. In addition, by providing security notifications and other important information, n/g CERTs can improve their visibility and build trust in their capabilities with constituents.

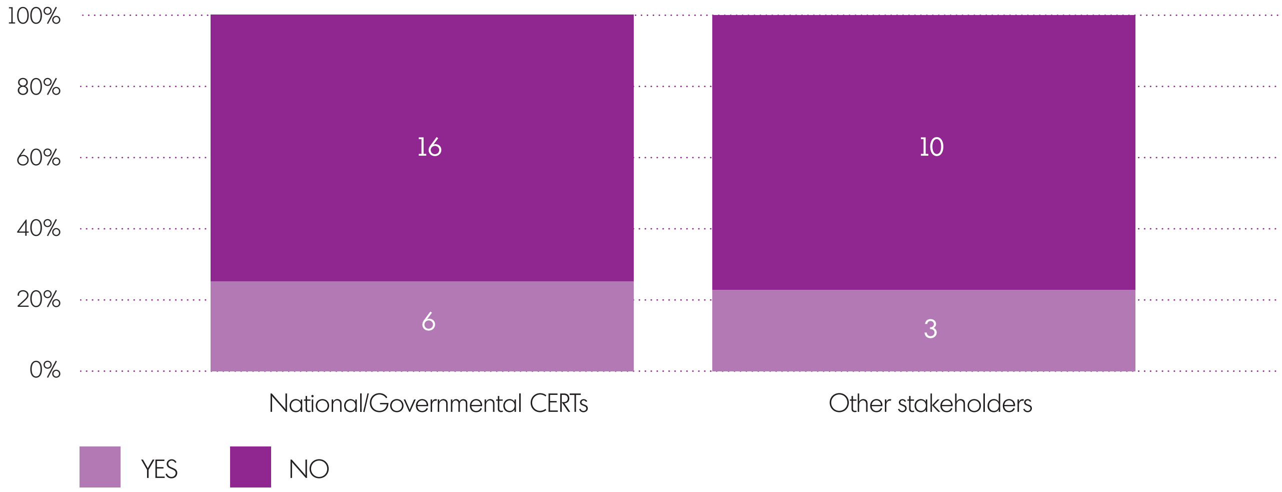
Most n/g CERTs do not provide all of their services to their entire constituency. Generally, they offer 'free' services (such as announcements and alerts that are not highly dependent on the target audience) to the public, including end users and other domestic constituents. Meanwhile, they often limit more resource-intensive services (e.g., incident response, vulnerability handling, artifact analysis, etc.) to specific constituents. These constituents generally, but not always, include an n/g CERT's government, public bodies, critical information infrastructure organisations, and sometimes other domestic CERTs. As a CERT-of-last-resort, n/g CERTs cannot and should not be expected to provide the same level of services to the broader public due to limited financial and human resources.

For now, three-quarters of n/g CERTs reported that they only provide 'typical'[20] CERT services and not 'new' CERT services (see Figure 3). Several n/g CERTs reported that they provide 'new' services ranging from legal

[20] www.cert.org/csirts/services.html

support to vulnerability coordination services or evaluation of the reliability of the Internet infrastructure in their country that are not in a typical n/g CERT's service portfolio.

Figure 3:
Services provided beyond traditional service portfolio



n=29 (16 n/g CERTs + 13 other stakeholders)

Cooperation can also offer n/g CERTs a way to improve their service portfolio capabilities. In particular, n/g CERTs can cooperate with other domestic entities that focus on cyber-security matters, such as national standards organisations, national cyber-security coordination centres, or security operations centres, to provide certain added-value, non-core services. The extent to which n/g CERTs can engage in this type of cooperation will depend on their mandate and the cyber-security-related bodies a Member State has established in its government structure.

"The service portfolio itself is still relevant; however, it is more a question of a shift of focus and how it is portrayed to the outside. CERTs need to reinvent themselves constantly – otherwise they themselves will become irrelevant in practice. While I think technical competence is key, legal competence is important as well. It is also important that this shift comes about without excessive organisational/managerial overhead. What we see is some CERTs trying to take on a bigger role but getting stuck in organisational/political issues."

An n/g CERT from a Member State

The following sections elaborate on these subjects and provide recommendations concerning the services of n/g CERTs according to the categories introduced above.

6.2 Proactive Services

N/g CERTs' main objective in providing proactive services is to reduce the number of cyber-security incidents by implementing preventative measures that secure the systems, processes, and people of the n/g CERT and its constituents.

While many n/g CERTs focused on providing reactive services when they were first established, almost all now also provide a number of proactive services. A strong majority of Member State n/g CERTs reported that they provide proactive services to their governments and public bodies and typically also to critical information infrastructure organisations in their country. A number of n/g CERTs also report providing proactive services to other domestic CERTs and some even offer these services to individual consumer and business end users, although CERTs sometimes limit the extent of the services they offer to their extended constituencies.

> ***"A lot of double work is going on by disseminating information on proactive announcements or technology watch by several CERTS and vendors, which is nowadays readily available on the Internet. A governmental CERT is, however, too broad for this and it would waste valuable resources."***
>
> CERT with ISP customer base

6.2.1 Gaps and recommendations

Gap:

General statistics on incidents solved by n/g CERTs are not made public in a number of Member States.

Recommendations:

These are short-term recommendations. There might still be some legal and procedural barriers in some Member States to disclosing the information.

- N/g CERTs should take steps to make anonymous and general incident report statistics available to the public.
- Policymakers can direct their n/g CERTs to do this through specific provisions in the mandate or other legislation, but should **allow n/g CERTs sufficient flexibility** to determine how to do this in a cost- and time-effective manner that takes into account valid reasons for not making all statistics about incident reports public.
- N/g CERTs should continue to share best practices among themselves for putting in place public-facing services, including the **dissemination of statistics.** ENISA might be a good platform for collection and evaluation of best practices.
- The collection and assessment of best practices would be further supported by agreement among n/g CERTs on a **common format of statistics** to be published. It is important that at least the type of an incident and solution status is included in the statistics.

6.2 Proactive Services

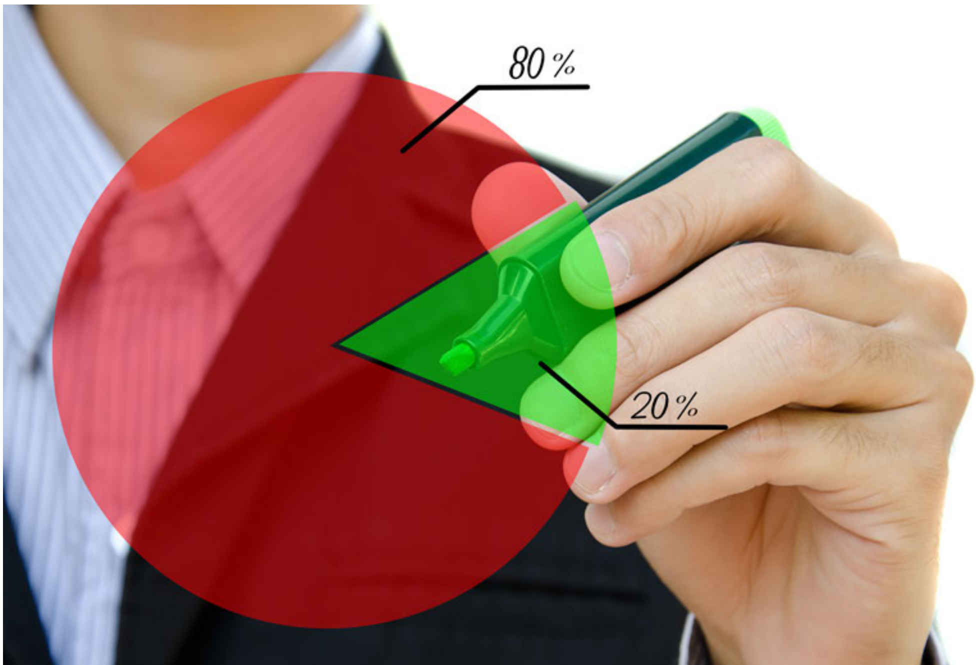
Gap:

CERTs do not offer services beyond the usual portfolio which might bring additional benefits to their constituents.

Recommendations:

These are short-term to medium-term recommendations. The intentions of n/g CERTs to introduce new services could be hampered by the lack of resources and mandate limitations.

- N/g CERTs should maintain **ongoing conversations with their constituents** – but especially their core constituents such as governmental bodies and CII organisations – about the services they provide and their utility. In addition, n/g CERTs should encourage internal staff discussion about their capabilities and speak with other domestic CERTs about their service portfolios.
- N/g CERTs should be willing to consider developing new services or tools if their discussions reveal tools or services that their constituents would find valuable that they are not offering, but should do so in an organised fashion that involves **expanding or changing their mandate to reflect these new service capabilities.** A careful cost–benefit analysis needs to be undertaken in this respect.
- This is an area that is well suited for informal communications between n/g CERTs; the exchange of information about tools and services that constituents in other countries find valuable should help n/g CERTs evaluate their capabilities and the tools and services they want to offer.
- The new services offered should be promoted by n/g CERTs, for example on their websites, in order to give more value and visibility to the n/g CERTs and its contribution to enhancing cyber-security in the respective Member State.
- N/g CERTs should be **aware of services already on offer by other CERTs and commercial vendors** and should take this into consideration when planning new services.
- It would be useful for n/g CERTs to consider consulting their counterparts in other Member States and subsequently **develop centres of excellence where individual n/g CERTs that exhibit expertise and leadership skills in certain areas or technologies can offer their expertise and services to other n/g CERTs.** Issues of national security need to be taken into account here, as well as the willingness of Member States to share certain information.



Gap:

There may be services provided by the n/g CERTs that are not considered as added value by the constituents, or may also be provided by other CERTs or commercial vendors.

Recommendations:

These are short-term recommendations. There should not be many obstacles to implementing them once the n/g CERTs have agreed with their constituents on the termination of the relevant service provision.

- N/g CERTs should discuss the value of their services with their constituents on an ongoing basis, and take care to ensure especially that key constituents such as government bodies and CII organisations find their services valuable. Heads of n/g CERTs will need to focus on developing and maintaining relationships with key players at constituent stakeholders based on trust and open dialogue about the n/g CERT's capabilities and services.
- N/g CERTs may reconsider whether to offer certain services that are not essential to fulfilling their mandate if they are given indications that they are not valuable to their constituents. Still, any reduction to an n/g CERT's current capabilities should be done only after careful consideration. This consideration needs to take account of the time spent by staff members on the provision of the given service.
- N/g CERTs should also try to maintain ongoing dialogues with other n/g CERTs about which services are most valuable to their constituents, and which their constituents find relatively less valuable.

6.2.2 Situation overview

Member State n/g CERTs offer the following proactive services to different extents:

- **Technology watch, announcements, and the dissemination and sharing of security-related information:** these services provide early warnings on threats or vulnerabilities and help a CERT's constituency protect its systems in a timely fashion. Member State n/g CERTs almost all provide proactive services, with a number of n/g CERTs reporting that they provide these services to almost their entire constituency.
- **Security and vulnerability assessments:** these help n/g CERTs' constituents to identify and address existing vulnerabilities in their infrastructure. Several n/g CERTs, including CERT.RO (Romania) and CERT-BUND (Germany) offer security assessments and audits on request to their constituents in government, other public bodies and critical information infrastructure organisations.
- **Providing guidelines on security configuration:** this service can help a CERT's constituency to harden systems to minimise the impact of an attack and reduce the residual risk. This service should leverage n/g CERTs' institutional knowledge and standing. N/g CERTs reported currently providing this service to different extents.
- **Providing intrusion detection services:** this helps a CERT's constituency to detect ongoing attacks or intrusions and initiate the incident handling process as soon as possible. By providing this proactive service, an n/g CERT can help its constituents limit an attack's damage. Several CERTs reported offering intrusion detection services to at least their core government and public body constituents.

6.3 Reactive Services

As previously noted, no IT system is perfectly secure; thus, vulnerabilities will be found and exploited. Member States need to put a comprehensive framework in place to ensure a timely and effective response to incidents. N/g CERTs are responsible for coordinating responses to incidents reported by their constituency, so they play a key role in this process. N/g CERTs should provide certain reactive services that help prevent a cyber-incident affecting a constituent from developing into a crisis. To prevent incident escalation, all parties that provide cyber-security services, including CERTs, need to respond in a timely and effective manner. Moreover, because private companies operate most critical information infrastructure, responses to attacks often require coordination between the government and private sector actors.

6.3.1 Gaps and recommendations

Gap:

Vulnerability and artifact handling are not fully provided by all CERTs.

Recommendations:

These are short-term to medium-term recommendations. Implementing them would require changes to the mandate and possibly additional resources.

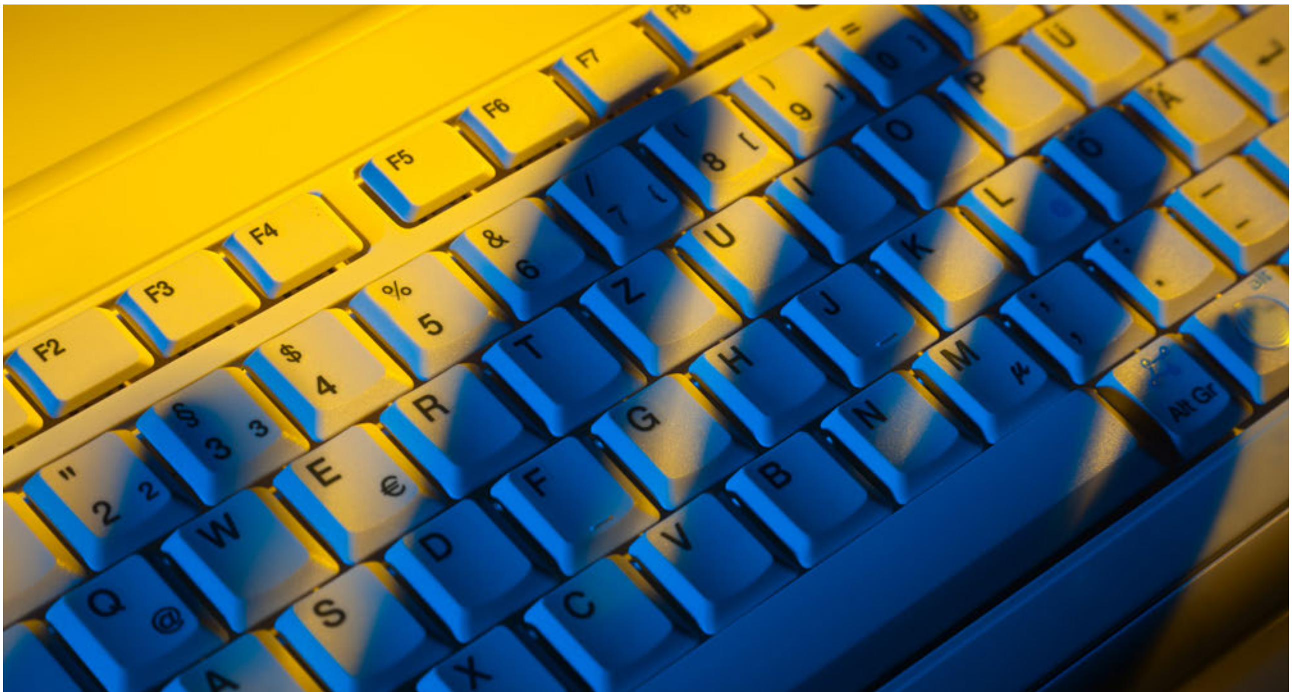
- Heads of n/g CERTs should work to convince policymakers and key constituents such as governmental bodies and critical information infrastructure providers in their country that having vulnerability and artifact handling capabilities is important to their serving constituents, including their governmental CERT functions.
- N/g CERTs should stress the synergies between these capabilities and the other services that they provide.
- N/g CERTs should take steps in the short term to discuss the extent to which constituents such as governmental bodies and CII organisations find it beneficial for the n/g CERT to have vulnerability and artifact handling services and use their input to build up a case to policymakers for receiving the necessary resources to support these services.
- N/g CERTs can also use ongoing informal discussions with their counterparts in other countries to gather anecdotes and data that support the importance of their having these services and the experience so far in providing them.
- Member States need to consider and secure additional funding so that n/g CERTs are able to deliver vulnerability and artifact handling. This may require either hiring new staff or reallocation of roles among staff of n/g CERTs with additional training.
- When deciding to offer vulnerability and artifact handling, heads of n/g CERTs should take into consideration whether or not such services are already being offered by the private sector or other CERTs and whether or not there is sufficient demand from the constituents.

6.3.2 Situation overview

The 'Policy Recommendations on Baseline Capabilities of National & Governmental CERTs' *report identified the following reactive services that n/g CERTs should provide (the extent to which they are already being offered varies across the region):*

- **Incident handling:** The ability of an n/g CERT to respond to incidents involving critical information infrastructure will hinge on it having an institutional structure that can support the necessary response. This makes it essential to have a clear mandate, to maintain clear lines of communication to the national executive, and to secure adequate financial and personnel resources. A strong majority of Member State n/g CERTs provide cyber-security incident handling to certain constituent subgroups, and especially to their governments, public bodies and critical information infrastructure organisations. A few n/g CERTs also reported offering these services to other domestic CERTs and end users.
- **Issuing alerts and warnings:** These services can be based on inter-CERT communications, incidents that occur in a CERT's constituency, and/or detected vulnerabilities. This is another service that the majority of n/g CERTs provide, with several offering these services to parties outside their core constituencies.
- **Vulnerability handling:** An n/g CERT must receive information about system vulnerabilities and be able to analyse it effectively in order to provide high-quality vulnerability alerts, counter-measures and expert incident handling. Member State n/g CERTs reported that vulnerability handling and vulnerability response coordination are among the reactive services they provide to their core constituencies.
- **Artifact handling:** Fewer n/g CERTs reported providing artifact handling services than other reactive services. In order to be able to provide high-quality alerts on new malware and other artifacts and to provide expert incident handling, the n/g CERT needs to receive information about and be able to analyse system artifacts.

Having a strong responsive framework is fundamental to n/g CERTs' mandate and responsibilities. Therefore, n/g CERTs must continue to develop their responsive capabilities, which means putting in place reporting thresholds, building adaptable response and recovery plans, and creating the coordination, information sharing, and incident reporting mechanisms needed for success.



6.4

Security Quality Management Services

An n/g CERT's security quality management services relate to its constituents' security management processes. The provision of these services recognises that an n/g CERT can provide specific and consistent support in matters such as security awareness building, CIIP business continuity or risk analysis. This, however, is influenced by the availability of resources at the n/g CERT and the nature and volume of special demands or requests from the constituents. Because of an n/g CERT's unique position and mandate, it is generally well placed to provide these types of services to some constituent subgroups.

An n/g CERT can build its capabilities in providing security quality management services by using and aggregating the data it gathers from its reactive and proactive services. It can use the data to report to its constituents on matters such as the most frequently reported incidents and newly discovered vulnerabilities. In addition, n/g CERTs typically have at least some cyber-security expertise in-house (e.g., incident handlers and technical experts), whereas other companies might have to hire external consultants for this type of work. Finally, as the CERT-of-last-resort that usually has a mandate as the country's official PoC, n/g CERTs generally have the authority and breadth of contacts to reach all relevant domestic organisations, including public and private sector actors, as well as the country's civilian population.

6.4 Security Quality Management Services

6.4.1 Gaps and recommendations

Gap:

The majority of n/g CERTs are still not involved in disaster recovery planning and business continuity management.

Recommendations:

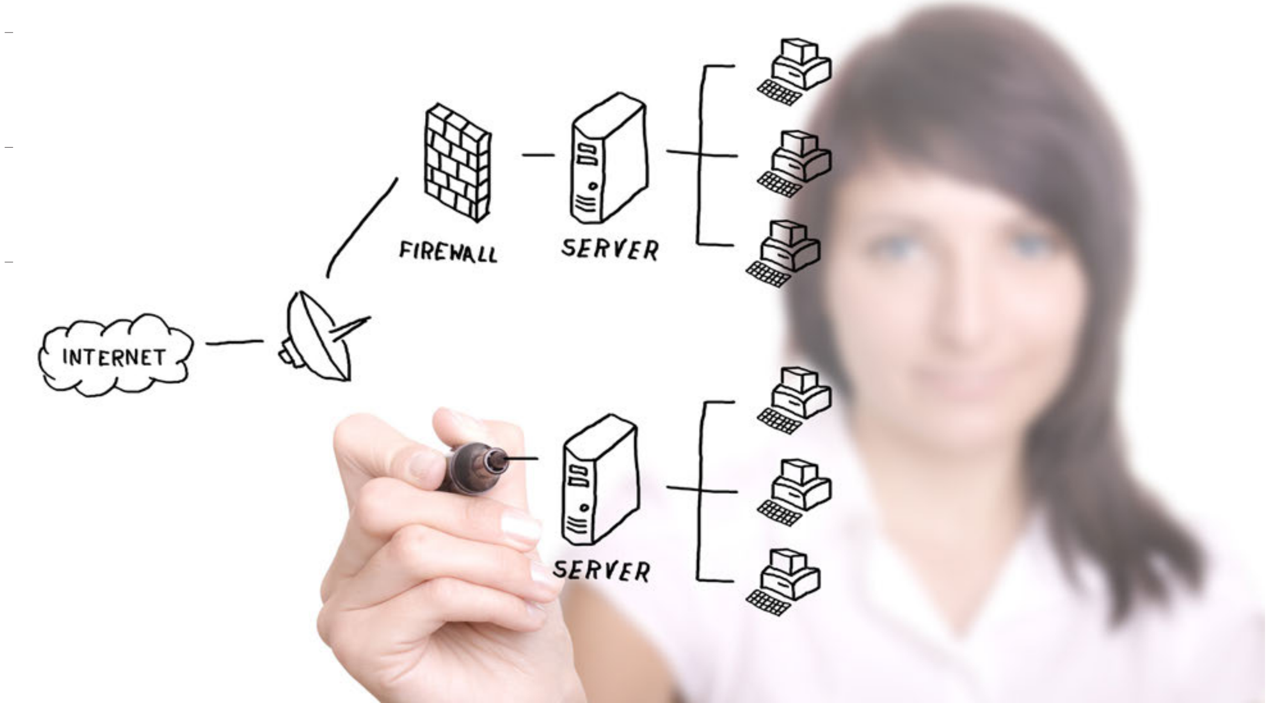
These are medium-term to long-term recommendations. The implementation of the recommendation may be challenged by the critical information infrastructure providers, especially from within the private sector.

- While maintaining an operational role in the incident handling process, n/g CERTs should consider, as an option, engaging in an **advisory role for mitigating the impact of large-scale incidents.**
- Should n/g CERTs consider this as an option, they can begin to establish their interest in participating in Business Continuity Management and Disaster Recovery Planning (BCM/DRP) by looking to take part in discussions at the government level about these matters where possible. To do this, n/g CERTs should work on developing a strong case about how their capabilities would benefit BCM/DRP efforts in their country and benefit their constituents, including governmental bodies that they serve.
- N/g CERTs might increase their visibility in BCM/DRP matters through cooperation or partnering with governmental agencies with an interest in these matters, such as national security agencies or telecom regulators.
- Over time, as n/g CERTs become more involved in BCM/DRP and risk analysis, they should update their service portfolio tables and request updates to their mandate as necessary.
- N/g CERTs should conduct an analysis on what impact the provision of BCM/DRM would have on their resources and work allocation.

6.4.2 Situation overview

N/g CERTs are providing a number of security quality management services to their constituents:

- **Awareness building:** An n/g CERT can play an important role in advancing knowledge and awareness about cyber-security, both within government and critical information infrastructure organisations, and with the general public. A number of n/g CERTs reported that they offer awareness-building services to their governments and other constituencies. Because individuals are often one of the weakest links in cyber-security, awareness building should be an important objective for n/g CERTs.
- **Education and training:** N/g CERTs can provide their constituents with valuable information and training on topics such as good practices in incident response or vulnerability management through workshops, courses, tutorials or exercises. A strong majority of n/g CERTs report offering some educational programmes and training exercises to their core constituents. There is considerable variation in the frequency with which n/g CERTs offer such education and training and in the subject matter covered. Several n/g CERTs noted that they offer training courses on an ad hoc basis and that their budgets do not allow for fixed curricula or mass training to parties other than their core government, public body, and CII organisation constituents.
- **Business continuity management and disaster recovery planning (BCM/DRP):** BCM/DRP is a key component of critical information infrastructure protection planning. Given their mandate and capabilities, n/g CERTs should be involved in the cyber-security aspects of BCM/DRP processes in cooperation with their constituents. Thus far, only some Member States' n/g CERTs have become involved in BCM/DRP. Several CERTs reported that they play active roles in conjunction with other government players in BCM/DRP efforts. Other n/g CERTs say that they take part in working groups or assist in making recommendations. Still, a significant number of n/g CERTs reported that they are not yet actively involved in BCM/DRP efforts in their country.
- **Risk management:** Traditional static risk analysis is becoming more dynamic. N/g CERTs can use the knowledge they build from providing reactive and proactive services to create a snapshot of situational awareness in its constituency. This type of information can then be used to support planning for and decision-making when a significant incident or crisis arises.



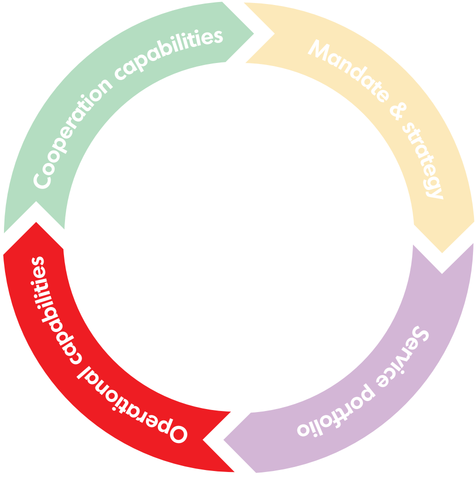
7

Operation

7 Operation

The operational capabilities cover technical and operational requirements an n/g CERT must comply with. There are four essential operational aspects of n/g CERTs:

- Human resources (team composition and operational mode)
- Infrastructure (communication services, logical security, physical security)
- Service delivery (service quality management in place)
- Business continuity.



An n/g CERT needs to have the appropriate staff, technologies and processes in place to fulfil its mandate, roles and responsibilities. If an n/g CERT does not have proper or sufficient resources, it will not be able to offer the services discussed in the previous chapter at a sufficiently high level. This chapter discusses essential operational needs of n/g CERTs such as staff and infrastructure as well as the operational capabilities that an n/g CERT must have to ensure that it can provide services of adequate quality to its constituency, even in the event of a cyber-crisis.

The operational requirements for an n/g CERT are based on its unique roles and responsibilities, which means that these operational requirements are very different from those of private or academic CERTs. N/g CERTs have a unique coordinating role in times of national crises that requires them to help protect national information infrastructures such as public communications networks or the availability of financial services. Therefore, it is essential that an n/g CERT remains operational under all circumstances. As a result, the business continuity of n/g CERTs is critically important. In comparison, most private or research organisations' CERTs have continuity requirements that depend on their missions or their hosting organisations' business cases.

7.1 Human Resources

An n/g CERT's human resources requirements depend on factors such as its mandate, regulatory and business drivers, the size of the country, and/or business hours.

7.1.1 Gaps and recommendations

The n/g CERTs now have sufficient staff to secure basic business continuity and provide core services. However, a constantly evolving IT security environment requires investing in specialised IT experts as well as in legal and public relations (PR) staff, while providing them with sufficient training.

Gap:

There is a perceived lack of legal and PR experts among the staff of n/g CERTs, which makes it more difficult to for them adapt to the evolving cyber-security landscape.

Recommendations:

These are short-term to medium-term recommendations. A barrier to implementation could be the level of salaries offered to legal and PR experts, as well as slow pace of cooperation with the educational sector regarding delivery of these experts.

- If the head of an n/g CERT believes that resources should be available, then he or she can work with policymakers to obtain funding for a legal and/or PR specialist. If funding is not likely to be available, then the head of the CERT should **consider working with their hosting organisation or private sector companies to discuss the possibility of sharing specialists** covering these areas.
- The issues should be addressed by encouraging the inclusion of IT security, public relations and law at an earlier stage in the curriculum of institutions of higher learning and universities. Member States should consider this as an objective and work with n/g CERTs to identify which issues should be considered for the curriculum.
- The n/g CERTs should foster their cooperation with LEAs and obtain training on legal and criminal matters from them, while the training provided by the n/g CERTs to LEAs have been in place for some time.

7.1 Human Resources

Gap:

N/g CERTs report difficulties in attracting highly specialised personnel, for example in reverse engineering and digital forensics.

Recommendations:

These are rather medium-term recommendations. Among the barriers to implementation could be budgetary restrictions in the public sector as well as legal provisions relating to temporary jobs in the Member States, especially in the sensitive area of national cyber-security.

- Recruiting strategies should showcase the most desirable aspects of working for them, which could include being at the **leading edge of cyber-security matters,** cooperation with other CERTs and domestic IT research institutes, or the opportunity to develop a variety of technical skills.
- This is another area in which either formal or informal sharing of best practices between CERTs could be beneficial, given that almost all n/g CERTs face a similar dilemma.
- There is scope for cooperation between n/g CERTs and universities specialised in IT issues, as the talented IT students may take temporary and part-time jobs at n/g CERTs in the roles of support staff. An arrangement could be considered whereby the students would agree to work for the n/g CERT for a fixed period of time (e.g. three to five years) after completion of their studies.

Gap:

Opportunities for 'deep-dive' technical training on cyber-security topics are still rather rare in Europe so it is important that, at the national level, heads of n/g CERTs and staff tasked with arranging training are proactive in finding appropriate technical training opportunities for their staff.

Recommendations:

These are short-term to medium-term recommendations. No major barriers in implementing the recommendation are expected as the costs of the technical training should decrease.

- N/g CERTs should always look for potential training opportunities through online courses or training sessions that are cost effective.
- N/g CERTs should also consider cooperative arrangements with other n/g CERTs, other domestic CERTs, or even certain constituents (in the case of ISPs and vendors) that can provide insight into certain technical issues, to limit costs while trying to obtain high quality technical training opportunities. Care should also be taken that the cooperative agreements with private sector constituents limit their allocation of human and technical resources to a necessary minimum.
- N/g CERTs across the region should look for efficiencies by opening their training sessions to other countries' CERTs, and by taking advantage of easily accessible training opportunities offered by other n/g CERTs.
- N/g CERTs should provide their wish-list of areas to be covered by the technical trainings to ENISA, so that it can take account of it when preparing workshops. There is scope for developing extensive training courses (like TRANSITS), on a wider range of topics.

Gap:

Although the n/g CERTs now provide or are shortly to provide 24/7 operational mode, this crucial facility is not always properly displayed on n/g CERTs' website.

Recommendations:

This is a short-term recommendation. It involves no obstacles to implementation.

- N/g CERTs should provide 24/7/365 contact information that is prominently displayed on their website and distinguished (if relevant) from the contact information to be used in regular business hours.

7.1.2 Situation overview

Team

According to the original 'Policy Recommendations on Baseline Capabilities of National & Governmental CERTs' report, Member State n/g CERTs are typically organised in a central team structure. The most important staff roles in an n/g CERT team are:

- Team leader/manager/coordinator, who:
  - Provides strategic direction for the team;
  - Is the authoritative representative of the n/g CERT and coordinates relations with other stakeholders;
  - Supervises and leads the team.
- Incident handlers who:
  - Provide incident handling capabilities by monitoring, analysing and responding to incidents;
  - Undertake technology watch, the dissemination of information and other tasks when no incidents are ongoing.
- Technical experts who can take on a number of roles, such as:
  - Vulnerability handling;
  - Technical writing;
  - Training;
  - Platform-specific support.
- Support staff who:
  - Carry out administrative tasks;
  - Monitor reports on events and incidents;
  - Undertake technology watch and the dissemination of information.

7.1 Human Resources

The 'Policy Recommendations on Baseline Capabilities of National & Governmental CERTs' report states that an n/g CERT needs to have at minimum a team leader and at least one incident handler to function. It is challenging to make broad statements about the (initial) right size of an n/g CERT, as many factors, including the CERT's mandate, its hosting organisation, and funding, influence its ideal staff size.

Even after surveying Member State n/g CERTs, it is difficult to identify best practices in terms of the sizes and structures employed by these CERTs and how they divide roles among their staff. The n/g CERTs' varying sizes, resources and responsibilities all make it difficult to draw firm conclusions about their sizes and structures. As a general rule, n/g CERTs uniformly seem to invest resources in ensuring that they have sufficient incident handlers and technical experts, although the number of these types of employees varies depending on the n/g CERT. Almost 90% of n/g CERTs reported that they have at least five full-time equivalents (FTEs), with a majority of n/g CERTs reporting that they plan to hire additional staff. Several CERTs noted that their sizes and structures necessitate that employees take on overlapping roles at times and that they exhibit flexibility.

An n/g CERT's staff's skill level is an important determinant of its capabilities, as the quality of services that it can provide will depend greatly on the personal and technical skills of its staff. The 2010 'Policy Recommendations on Baseline Capabilities of National & Governmental CERTs' report listed strong communication skills and cyber-security knowledge as among the most essential competencies for staff members, with technical expertise especially needed at the manager level.

Some n/g CERTs reported that they find it challenging to find sufficient experienced and qualified staff, especially on the technical side. This is related in part to the fact that public sector salaries often cannot compete with what a technical expert in a 'CERT relevant' area could earn in the private sector. One option to consider, however, would be to create special positions for experts that allow an n/g CERT to pay them a competitive salary. Still, some respondents, especially from smaller n/g CERTs, said that it is hard to provide employees with the chance to develop areas of expertise – a factor that could hold back a CERT's overall capabilities. In addition, several n/g CERTs mentioned legal support as a human resource skill that their team lacks.

Operation mode

The original 'Policy Recommendations on Baseline Capabilities of National & Governmental CERTs' report states that the minimum staff size for an n/g CERT is three FTEs. According to this report, an n/g CERT can deliver typical office-house service, but not 100% availability, with three staff members. It further states that an n/g CERT that wants to provide a 24/7 work-shift needs at least 5 staff members.

If an n/g CERT does not have 24/7 availability, it will become more challenging for the CERT to cooperate internationally (made even more challenging by time differences) and to provide timely incident response services. A CERT's incident handling service is the most important service that a 24/7 operation should provide. Incidents impacting CII may need to be resolved before the next morning to avoid catastrophic consequences.

While recognising that n/g CERTs face funding and resource limitations, it is extremely important that they are at minimum reachable 24/7/365 by their constituents and domestic and international partners. N/g CERTs are responsible for protecting their government's critical information infrastructure and serve as a CERT-of-last-resort for their entire constituency, which makes it essential that they are available 24 hours a day, 365 days a year. According to the 'Policy Recommendations on Baseline Capabilities of National & Governmental CERTs' report, it takes a minimum of 6 to 8 staff members for an n/g CERT to ensure 24/7/365 availability.

Member State n/g CERTs generally maintain relatively typical office hours (e.g., 8 a.m. to 5 p.m. Monday to Friday) and supplement these office hours with emergency contact availability for non-office hours. Almost all n/g CERTs report that a staff member can be reached outside normal office hours either by an emergency telephone number or through a dedicated operator that monitors calls. This suggests that Member State n/g CERTs understand that they cannot have 'dead times' when they are completely unavailable. If there are two or more n/g CERTs in the Member States, each CERT can act as a backup for the other and vice versa.

Depending on its service portfolio, work structure and responsibilities, an n/g CERT's team needs to be reachable either in office or through 'on-call duty'. Either way, it is critical that an n/g CERT be able to guarantee quick response times, especially for incident reports. This means that each team will need a number of specialised technical experts available to provide services such as artifact handling and security assessment. If an n/g CERT uses shift work or on-call duty schedules, special procedures and requirements, such as escalation procedures, maximum response times, and backups, must be put in place.

7.2 Infrastructure

N/g CERTs face stringent requirements concerning confidentiality, their integrity and infrastructure availability because of:

- the role n/g CERTs play in crisis situations (e.g. large-scale cyber-attacks);
- the confidentiality of the information an n/g CERT processes and stores (records of incidents, CII vulnerabilities, etc.);
- the critical nature of the infrastructure that an n/g CERT helps to protect (energy, healthcare, communication networks, etc.).

7.2.1 Gaps and recommendations

The n/g CERT should ensure high availability of their communications services by avoiding single points of failure and have at least several means for being contacted and for contacting others. Furthermore, the communications channels should be clearly specified and well known to the constituency and cooperative partners.

Gap:

Most n/g CERTs reported that they provide several different ways for their constituents to contact them. They provide this information both publicly on their website and also through private communications with their constituents. They often use the services of more than one provider as a backup. But there is an indication that n/g CERTs could be more proactive in utilising social media platforms for less sensitive information.

Recommendations:

This is a short-term recommendation, which depends on n/g CERT teams developing clearer communications strategies.

- N/g CERTs should work to provide as many secure means of contact to their constituents as possible. Especially for less sensitive matters such as news dissemination or contact information updates, n/g CERTs should consider whether newer means of communication such as social media (Facebook, Twitter, LinkedIn) might serve their purposes. Contact information for n/g CERTs should be clearly stated and prominently displayed on their websites, and constituents should be proactively informed of changes to contact information or new ways of contacting an n/g CERT.

7.2.2 Situation overview

Communication services

N/g CERTs generally do not have direct access to the systems affected by a cyber-security incident, so they must be able to rely on the telecommunications services they use, including telephone and broadband network connections, to receive information about the incident to begin analysing it and coordinating its handling. This reliance on external communications systems and infrastructures is a factor that n/g CERTs have to take into account for almost all the services they provide.

An n/g CERT must have at minimum telephones (fixed and mobile) and an Internet connection (for VoIP, email and the Internet) to carry out its responsibilities. Generally, these fundamental means of communication will be those used most often by the CERT. Typically, n/g CERTs offer their constituents several ways of contacting them. N/g CERTs provide contact information and means of contact on their website or through direct communications with their constituents. Some n/g CERTs have preferred ways that their constituents should contact them, even if they offer a number of means of contact. Generally, the PGP-protected email is the most common method of communication.

The security of information that is being exchanged between n/g CERTs and their constituents is also important, which is why n/g CERTs should provide details for signed and encrypted email (e.g., PGP key). In addition, the team's website should provide a secure means of communication (e.g., an https-protected incident reporting form). Three-quarters of Member State n/g CERTs reported that they use PGP encryption to ensure the privacy and security of their electronic communications. N/g CERTs also report using other solutions to various extents, such as encrypted network backbones, full-disk encryption, crypto-communication; and S/MIME certificates, and secure portals are being considered.

Availability is also something that n/g CERTs have to take into account. No single means of communication has guaranteed availability; backup communication channels should always be available and announced. If possible, different means of communication should not be run over the same physical carriers in the event that a single point of failure in the communication infrastructure makes a CERT unavailable to its constituents.

Logical security

Because of the sensitive nature of cyber-security incidents and vulnerabilities, n/g CERTs possess and store a significant amount of confidential information. The 'Policy Recommendations on Baseline Capabilities of National & Governmental CERTs' report mentioned that, in addition to security measures for communication channels, logical security controls should be implemented to protect the confidentiality and integrity of information, such as:

- An internal information security management framework and policy to provide the security strategy and authorisation to implement controls over the:
  - information classification scheme, shared with the n/g CERT's constituency and partners;
  - password policy;
  - access management policy;
  - etc.
- Integrity controls (e.g., hash comparison) to prevent unauthorised changes;
- Confidentiality controls such as encryption.

Additionally, all logical security measures should be managed by the n/g CERT itself, in order to ensure the data's confidentiality and integrity.

Physical security

The importance of physical security for an n/g CERT can be easily underestimated given that CERTs deal primarily with cyber threats. That said, because n/g CERTs deal with sensitive information from governments and individuals, they must take adequate measures to physically secure their premises. The fact that n/g CERTs are typically in possession of sensitive information from other countries makes security of premises even more important.

Respondents from Member State n/g CERTs were somewhat hesitant to discuss the specifics of the physical security steps that they have implemented, but emphasised that their physical security measures are in accordance with national and EU standards. A number of n/g CERTs reported that they have implemented measures such as controlling access to their premises through security access card control, hiring 24/7 security guard staff, and only allowing supervised visits to their facilities. Several n/g CERTs simply responded that information about their physical security measures is confidential and sensitive and cannot be divulged.

7.3

Business Continuity

A core role of n/g CERTs is to help mitigate the impact of attacks against their country's infrastructure. Having and demonstrating the ability to ensure the resilience of its own infrastructure also helps the n/g CERT by making it appear more competent to its constituency; this can increase the levels of trust placed in the n/g CERT by its constituents. In terms of operational requirements, ensuring continuity is a general issue that covers many important aspects of an n/g CERT's operations.

7.3.1 Gaps and recommendations

An n/g CERT has to ensure the resilience of its infrastructure in the face of attacks, and the team needs to have a plan for ensuring service continuity, as well as relevant skills.

Gap:

Some CERTs continue to find it challenging to hire sufficiently skilled staff to address their business continuity needs.

Recommendations:

This is an ongoing recommendation, as the need to review and update business continuity plans will remain a priority.

- N/g CERTs should ensure that they have good systems in place for managing incident reports and that they will be able to access their infrastructures and communication services even in the event of an attack. Where possible, n/g CERTs can look to international best practices for guidance on best ensuring continuity.

7.3.2 Situation overview

Ensuring continuity

Managing incoming requests and being able to correctly distribute them between staff (even across work-shifts) is an important part of ensuring continuity. A second is having 24/7/365 availability that allows constituents to call in incident reports at any time. A third aspect of ensuring continuity is having the ability to cope with the loss of critical communications channels and operational elements such as email or information services (WWW, FTP, etc.). Not having access to these communication channels could mean that an n/g CERT is unable to provide specific services in a timely fashion and mean that it fails to meet contractual requirements and/or services as specified in SLAs. N/g CERTs should aim to avoid this to the extent possible by creating redundancy in their infrastructures and by having a variety of communication channels, as discussed previously.

It is also important that n/g CERTs invest in the ongoing training of their staff to ensure that they possess up-to-date knowledge (which is an investment in continuity in the longer term) and that their staff have the chance to engage in regular exercises. Eighty percent of CERTs reported that they believe that their staff have sufficient training opportunities (except for technical deep-dives) through a variety of training internal and external courses. TERENA-TRANSITS courses in particular were mentioned by a significant number of CERTs as a training programme that they use.

7.4 Provision of Services

N/g CERTs should try to identify and monitor their most important key performance indicators (KPI) to provide a framework for evaluating the quality and performance of their services. The indicators they choose should be relevant to their key mission objectives and weighted according to the importance of the service to which they relate.

Examples of various quality parameters can be found in reports or frameworks for information security metrics. The KPI that were mentioned in the 'Policy Recommendations on Baseline Capabilities of National & Governmental CERTs' *report are:*

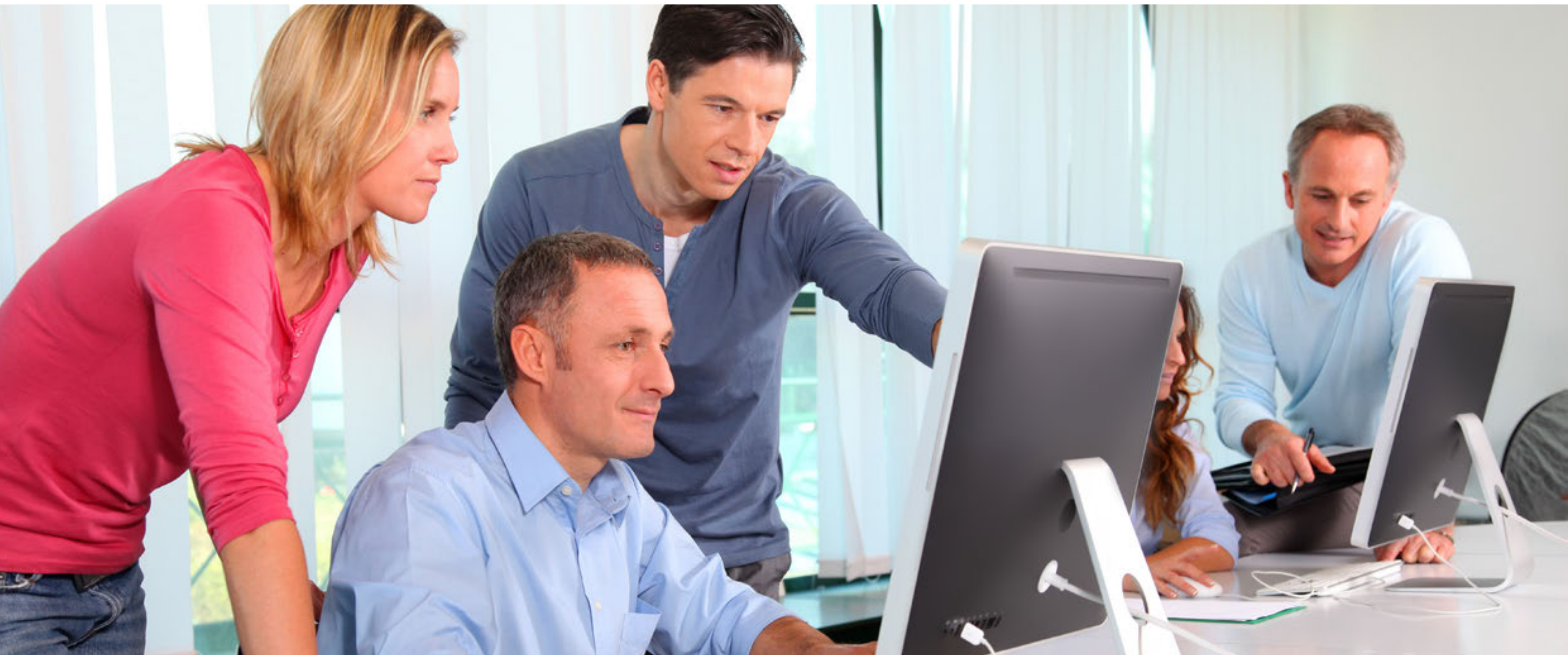
- response times for service events (e.g., incident, vulnerability report) and/or priority scheme;
- level of information provided for service events (short-term);
- time-to-live for service events;
- level of information provided on the longer term (reports, summaries, announcements).

Specific examples:

- **Follow-up on high-priority incidents:** Every high-priority incident will be acknowledged within two hours. Analysis on such an incident will start within one hour of when a report of an incident is received.
- **Follow-up time on vulnerability reports for all non-urgent vulnerabilities:** The n/g CERT should follow up with a constituent that makes such a report within two working days of the initial report.

7.4.1 Gaps and recommendations

Although funding is sufficient for n/g CERTs to secure provision of core services, for provision of all services from a typical CERT service portfolio and even introducing new ones in line with demands from the constituents, it is desirable that the n/g CERTs look for additional sources of funding complementing the national budgets.



Gap:

N/g CERTs often rely entirely or almost entirely on state funding with few or no additional resources.

Recommendations:

These are ongoing recommendations. A barrier to implementation might in some cases be mandate limitations, which do not allow n/g CERTs to seek additional resources apart from state funding.

- N/g CERTs can consider several possibilities to obtain additional funding. For example, an n/g CERT could apply for funding through EU projects. Alternatively, many n/g CERTs have valuable knowledge and capabilities, and could try to sell training, consulting or research projects.
- N/g CERTs have to **pursue alternative funding sources** while fulfilling their mandate and where possible after having discussed the decision to seek alternative funding with both policymakers and key constituents such as governmental bodies and CII organisations.
- Securing adequate funding is an issue that all n/g CERTs face, so where possible they should seek to share their experiences and best practices with each other.

Gap:

Some constituents claim that a governmental-type of CERT is rather secretive when it comes to providing data.

Recommendations:

These are medium-term to long-term recommendations. The implementation might be compromised by the insistence on state secret rules applied by the governmental type of CERT.

- The constituents should discuss with n/g CERTs having the governmental CERT role the need for them to be more open to share and transfer data on incidents affecting the cyber community on the national level.
- The governmental CERTs are encouraged to consider non-disclosure agreements with constituents (mainly other CERTs) on the scope of information for the exchange of data.
- Technical aspects of automated data exchange should be addressed in working groups possibly established by ENISA, FIRST, TF-CSIRT or other CERT initiative.

7.4.2 Situation overview

Supporting processes and tools

N/g CERTs can employ several supporting processes and tools to help them increase the efficiency and maturity of their service delivery.

First, n/g CERTs should have an incident recording and tracking system (aka a ticketing system) to ensure service delivery. Having this in place allows the CERT to create tickets that are associated with incidents. As the incident handling phase progresses, information can be added to the ticket, which creates a formal audit trail and incident log.

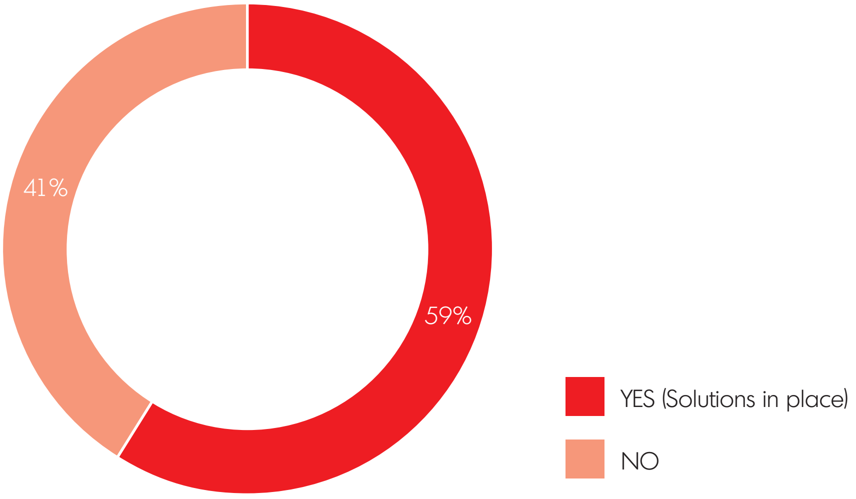
7.4 Provision of Services

Second, defining the standard procedures that apply to the services that an n/g CERT provides helps it to ensure that processes are executed. These procedures are also a key to maximising a CERT's effectiveness and efficiency.

Third, a workflow management system can queue and centralise information coming from different communications channels, as well as allowing for predefined workflows to be followed in the handling of incidents. This allows for proper monitoring of the status of incidents, facilitates hand-over between shifts, generates reports, and ensures that standard processes are followed. Ideally, service delivery will be defined in an SLA, along with its costs. At the very least, an n/g CERT needs to publish its most important KPI.

Nearly 60% of n/g CERTs reported that they have service management processes in place (see Figure 4). That said, a majority of Member State n/g CERTs also indicated that they still have work to do in terms of implementing service management or quality systems and processes to improve on their performance. A number of n/g CERTs simply reported that they have no such service management quality systems in place. Some said that they are in the process of developing such policies, and others follow their government's general guidelines. Only a few n/g CERTs report having developed their own service management quality systems.

Figure 4:
Service quality management systems in place



n=22 n/g CERTs

Member State n/g CERTs use a variety of sources of information for good practices, with ENISA reports and CERT/CC documents being mentioned most often as sources employed for procedures on handling critical incidents. Other sources of best practices taken into account by CERTs include: NATO[21] procedures, US-based NIST[22] special publications, best practices from other CERTs, and internally developed procedures.

[21] http://www.nato.int/cps/en/natolive/index.htm

[22] http://www.nist.gov/index.html

8

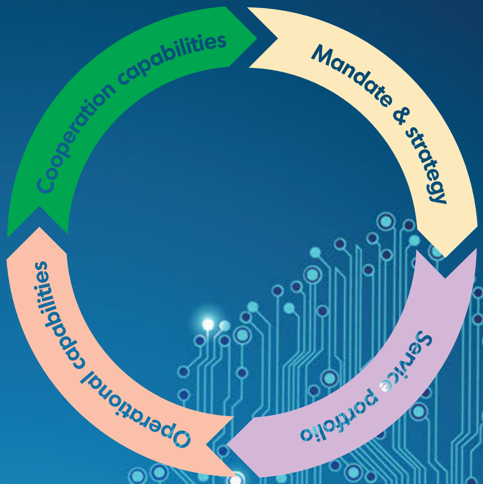
Cooperation

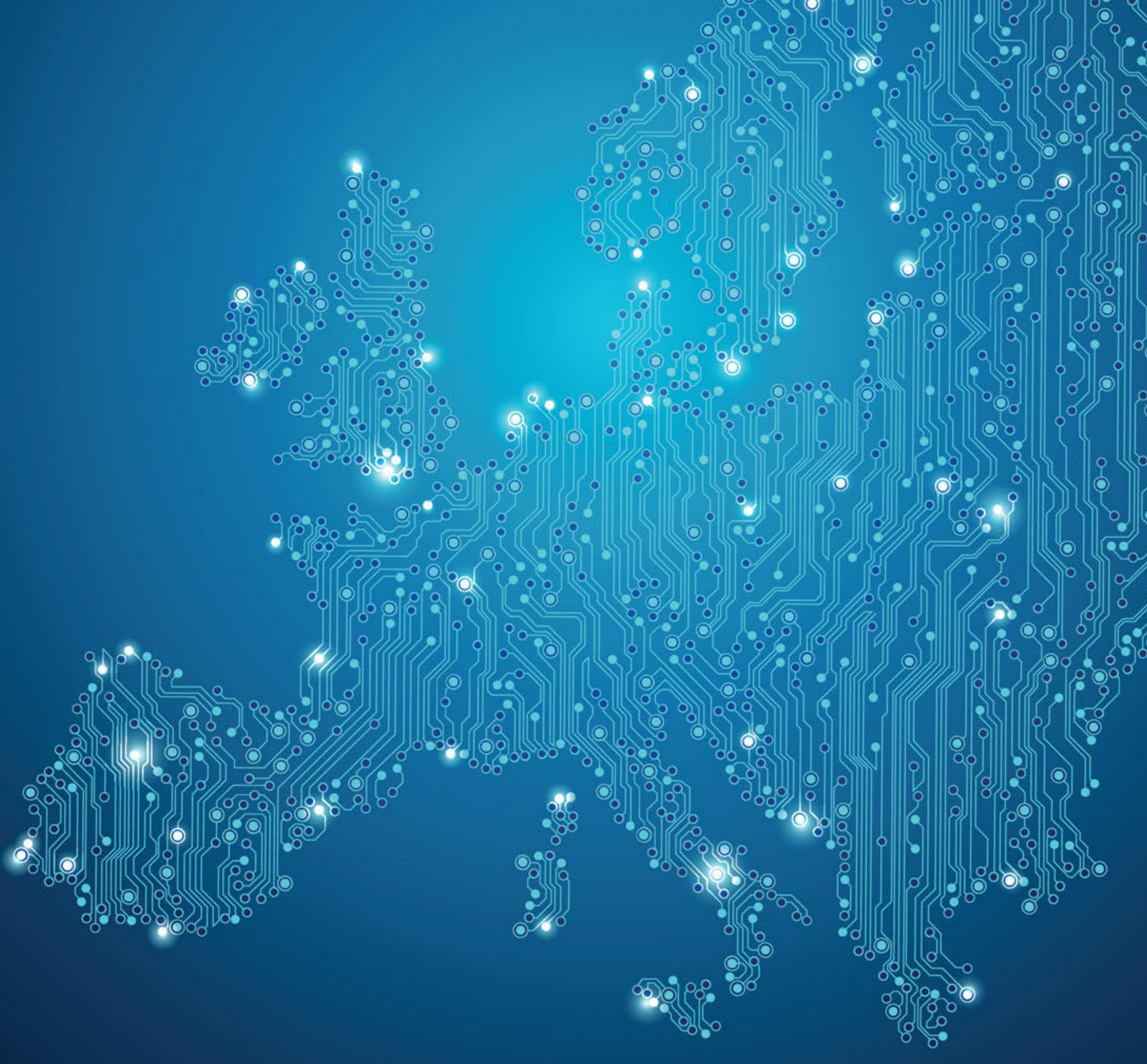
8 Cooperation

8 Cooperation

Cooperation capabilities refer to requirements with regard to information sharing with other teams as well as with other stakeholders at national and cross-border (international) levels that are not covered by the previous three categories of capabilities. In this regard there are three crucial elements for n/g CERTs:

- trust and trust building;
- quality and sustainability of information and reaction;
- common terminology and schemes.

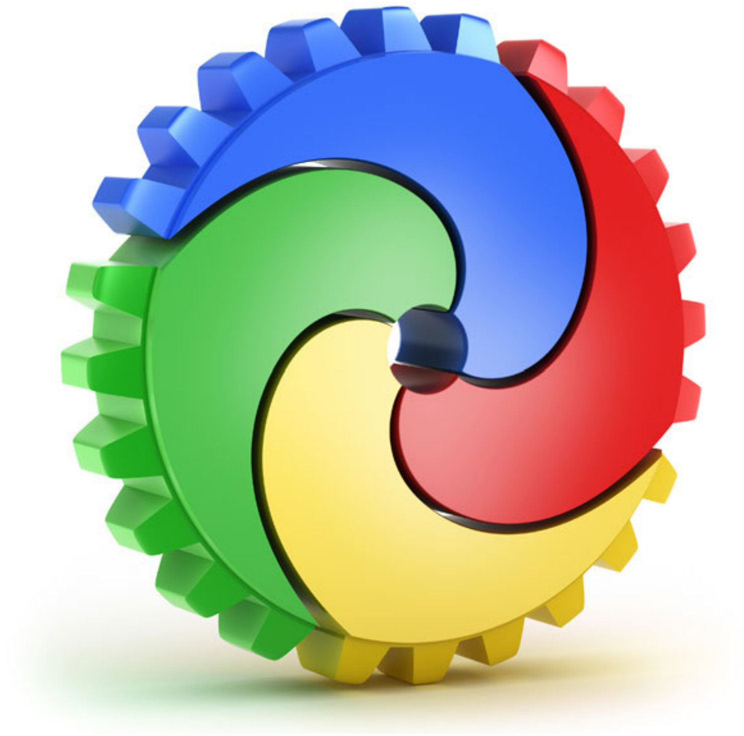




8 Cooperation

A security breach in one network can very quickly become a threat to other networks and devices connected to those networks. The ease with which cyber-attacks can infect multiple networks and spread among multiple devices demonstrates that although ICT infrastructure may be owned and operated by independent entities in a given country (as well as by bodies outside the country such as multinationals), ultimately the infrastructure is interlinked and often interdependent. This is also true on an international level. The ease of global travel and the proliferation of cross-border ICT business processes mean that national networks are also interlinked and interdependent on each other. Consequently, a vulnerability or security breach in one country quickly becomes a threat to other countries.

With this in mind n/g CERTs are well positioned to serve as a point of national contact for outside parties. The aim is to have a central point of contact in a country to oversee all networks and stakeholders, so that isolated vulnerabilities and threats can be addressed before proliferating. And when breaches do occur on a national level, there can be a central point of contact that can coordinate a response. Coordination on this level, however, comes with its challenges. The effectiveness of an n/g CERT's activities can often be dependent on its authority to enforce security requirements, and the extent to which its powers extend to all members of its constituency. And even with the requisite powers, coordinating the various stakeholders can be a challenge not only in terms of the technical and organisational barriers that can arise, but also in terms of establishing the trust and confidence among its constituencies needed to ensure their cooperation.



8.1 National Cooperation

An n/g CERT coordinates security incident handling and responses on national level between a number of stakeholders that are deemed to have a critical role in the nation's ICT security. Stakeholders range from other CERTs to offices of the public administration, educational institutions, private businesses, and other critical infrastructure entities. In many cases n/g CERTs also cooperate with military and intelligence authorities. The cooperation can take place on an advisory level, or involve more active enforcement of security measures on its constituency. To date, most n/g CERTs operate on a voluntary model, whereby they can issue statements and provide guidance, but stop short of actually imposing any security requirements on their constituents. Enforcement in Member States is mostly left to existing regulatory and law enforcement authorities when clear violations of law take place.

8.1.1 Gaps and recommendations

N/g CERTs have been empowered with a mandate, which sets the framework for both national and cross-border cooperation. In order to streamline and facilitate the cooperation on the national level the awareness of the n/g CERT among cyber-security stakeholders should be promoted. At the same time it is useful to consider enhancing powers of n/g CERTs to require constituents such as ISPs to handle incidents when requested by the n/g CERT (at the operational level). Also, n/g CERTs should be able to gain access to statistical data on reporting of incidents that is collected by the national regulatory authorities, and possibly contribute to the overview.

8.1 National Cooperation

Gap:

One major obstacle to national cooperation is the fact that national stakeholders are still not sufficiently aware of the existence of the n/g CERT and its powers. Raising awareness about the existence and responsibilities of n/g CERTs is the responsibility of the n/g CERTs themselves. Heads of n/g CERTs should allocate resources for raising awareness.

Recommendations:

These are short-term to medium-term recommendations. The implementation may require hiring a specialised PR agency, as this capability is often not in place within n/g CERTs or their hosting organisations.

- Firstly n/g CERTs should have, or create, a **database of key stakeholders** and with that list begin to organise outreach programmes. Such programmes can be implemented in a number of ways. One approach could be through so-called cold introductions, where n/g CERT heads take it upon themselves to call or visit stakeholders directly and make introductions.

- Since stakeholders can often be busy, the n/g CERTs should have targeted presentations, in the form of PowerPoint slides or other documents that clearly and concisely explain the CERT responsibilities. Presentations should outline teams' responsibilities as concisely as possible, so as not to take up too much time, and focus on the key elements of the n/g CERT's responsibilities as a lead-in to potential further discussions if necessary.

- Publishing articles on national security threats in media sources can also be an important tool for raising awareness among a wider audience. N/g CERTs should be familiar with the leading media outlets, both mass market and speciality industry publications where they can submit opinion pieces related to cyber-security.

- Delivering presentations at industry events and conferences should also be a goal. N/g CERTs should familiarise themselves with the most popular and relevant industry events and volunteer to present at them.

- These domestic campaigns closely involving national media sector should run in parallel to participation in regional or international events. It is important that n/g CERTS **raise awareness regionally and internationally**, too. Presentations on best practices are always in demand at international conferences. N/g CERT heads or technical staff should be willing to share best practices and local experiences as part of an international forum as a means to raise awareness abroad.

8.1 National Cooperation

Gap:

There is a need to enhance powers of the n/g CERT to require operators to report incidents.

Recommendations:

These are medium-term recommendations. The implementation might be delayed by lengthy legal procedures and reluctance on the part of service providers.

- Policymakers in Member States should begin considering whether it would improve their n/g CERT's capabilities and their overall cyber-security strategies to give the n/g CERT the authority to require operators active in their market to report certain types of cyber-incidents that occur on their networks to the n/g CERT.
- N/g CERTs need to take the initiative to develop long-term cooperative partnerships with operators/ISPs in their markets to allay operator concerns about their having this authority and to begin to develop standard protocols for the reporting of incidents. These **cooperative partnerships** may also form the basis for informal channels of communication between n/g CERTs and operators that can be used for informal discussions and sharing of information.
- N/g CERTs should share information with each other about what approaches have worked in convincing operators to report incidents, and consider engaging telecom operator advocacy groups about the rationale for providing n/g CERTs with the authority to require operators to report certain types of cyber-security incidents.
- As operators are obliged to report network security breaches to national regulatory authorities, provisions should be made to ensure that n/g CERTs get easy access to this information. This would also eliminate double reporting for service providers and network operators.

Gap:

Service providers and CII operators are often reluctant to provide their data for fear of data disclosure to competitors.

Recommendations:

These are long-term recommendations. Their implementation will depend largely on confidence-building measures between n/g CERTs, service providers and operators.

A number of steps can be taken to address this issue:

- There is room for greater participation between n/g CERTs, ISPs and telecommunications network and CII operators in working groups. Such working groups are not yet active in a number of countries; or, in many cases where there is cooperation, it is more informal. Formal working groups with targeted agendas that are designed to air concerns over data protection would **facilitate a dialogue between n/g CERTs and service providers with the stated aim of demonstrating how n/g CERTs can be trusted to protect competitive information**.

- Signing memoranda of understanding or other protocols on non-disclosure between n/g CERTs and service providers/network operators could also be a way of accomplishing the task.

- Aside from improving relations, regular participation in working groups which are organised with formal agendas can be an important tool for gathering feedback from constituents on the performance of n/g CERTs and identifying areas for improvement. In other words, **n/g CERTs need to hear directly from service providers what measures they expect the n/g CERTs to take in order to ensure data is not compromised**. But it is up to n/g CERTs to take this initiative and encourage service providers and CII operators to cooperate, as well as to engage data protection authorities who act as overall guardians of personal data.

- Technical staff from n/g CERTs could play an important role in such working groups, demonstrating security policies and how sensitive information is protected. Details on the methodologies involved could help build trust and demonstrate to service providers that their competitive information will not be compromised.

- This issue should be included on agendas for international CERT conferences too. Sharing of best practices and critical success factors on protecting competitive information can be useful for other n/g CERTs that are still working to build up confidence in the market about their ability to protect information.

Gap:

Cooperation with law enforcement authorities can be one-sided, in cases where LEAs are not in a position to share information, particularly during an investigation. While certain legal barriers need to be respected, there are ways that n/g CERTs can keep lines of communication open and work together in areas of mutual interest.

Recommendations:

These are long-term recommendations, and their implementation might be hindered by strict legal constraints on the type of data that LEAs are allowed to share. Therefore, the implementation will have to be done on a 'best efforts' basis.

- Maintaining relationships based on written agreements should continue, as long as such agreements have room for flexibility to evolve and change so that all parties can respond to changing security technologies, vulnerabilities and threats.
- Heads of n/g CERTs should meet regularly with LEA officials to **discuss trends in cyber-security and review and share information about potential risks or threats** that should be brought to each other's attention.
- Both n/g CERTs and LEAs should invest in prevention. To do this, they can maintain open lines of communication about potential areas of concern so that problems can be identified in advance.
- LEAs could benefit greatly from the technical expertise available at n/g CERTs. Participation in joint workshops where n/g CERTs could provide technical guidance and expertise to help LEAs in their investigations could be a good starting point. This way even if n/g CERTs cannot actively participate in the investigations, they can provide expertise that can aid the LEAs, indirectly assisting the investigation.
- There is room to improve international relations with law enforcement officials, where law permits. This is particularly important to **address cyber threats where criminals may use infrastructure in one country to launch an attack against networks and devices in other countries**. Improved relations could be achieved through written agreements where cooperation is clearly outlined and in accordance with relevant laws, or through voluntary informal communications, again in line with relevant laws.

8.1.2 Situation overview

Constituency

As most CERTs operate on a voluntary model, the effectiveness of their operations is very much dependent on cooperation from its constituency. Without cooperation from its constituents, the CERT's efforts can be made ineffective. The cooperation must exist in two directions, with constituents receiving and abiding by guidance coming from the CERT and at the same time providing information and guidance to the CERT which is needed for the CERT to perform its basic duties.

A CERT's ability to effectively monitor and respond to incidents depends on how much constituents cooperate in terms of sharing data and other relevant operational and technical information about their network operations. Often constituents will naturally be reluctant to share some information, as it may compromise competitive secrets and could potentially violate data protection rules, depending on how the rules are interpreted and enforced. Consequently as long as the relationship remains voluntary, the power of a given n/g CERT will be limited to a certain extent. Defining a clear mandate and potentially expanding an n/g CERT's powers to collect more clearly defined data from specific types of organisations could help overcome this barrier.

To date n/g CERTs have limited or no powers to require constituents to implement measures. The vast majority of n/g CERTs work in this area on a voluntary model. Feedback from n/g CERTs indicates this model works well within the framework of their overall responsibilities. When action needs to be taken and a particular requirement enforced, they are willing to cooperate with law enforcement authorities to ensure compliance when any relevant laws are broken and require enforcement. The voluntary model should continue to be pursued. As cyber-security laws evolve, they might find a place for specific enforcement powers to be granted to n/g CERTs, but this should be clearly outlined so as to avoid conflicts with existing enforcement authorities.

Internet Service Providers / Telecommunication Network Operators and other CII operators

Networks belonging to telecom operators, ISPs and other CII operators require a high level of security and constant monitoring due to the size of their networks and the dependency that consumers and businesses have on the infrastructure and services running on the networks. Such networks can be the target of cyber-attacks and at the same time can be exploited to launch attacks. If CII networks are compromised, there can be significant consequences to a country's national security and disruptions to the population's day-to-day communications needs. With this in mind, the relationship between n/g CERTs and CII operators can require a higher level of cooperation. In practice, this can be challenging. As with any private-sector company, TelCos, ISPs and other CII operators can be reluctant to share data with n/g CERTs for competition reasons, as well as concerns regarding compliance with regulatory conditions. Additionally, security measures recommended by n/g CERTs could have a direct impact on a company's costs and resources.

N/g CERTs across Europe indicate that they have a strong relationship especially with telco operators and ISPs when cooperation is needed. While n/g CERTs may not be able to require operators to implement a specific security measure, n/g CERTs have found that operators are usually willing to cooperate when an incident arises. While relationships are voluntary, it is common for n/g CERTs and TelCos and ISPs to have written agreements detailing the cooperation.

Relations between n/g CERTs and ISPs, telecommunication network and other CII operators remain voluntary. Nonetheless, it is common for n/g CERTs throughout the EU to establish formal written agreements that outline the nature and conditions of the voluntary relationship. Such guidelines ensure clear expectations and avoid potential conflicts over handling of incidents and sharing of information. This cooperation overall is working well and n/g CERTs report an adequate level of cooperation within the framework of their given mandate.

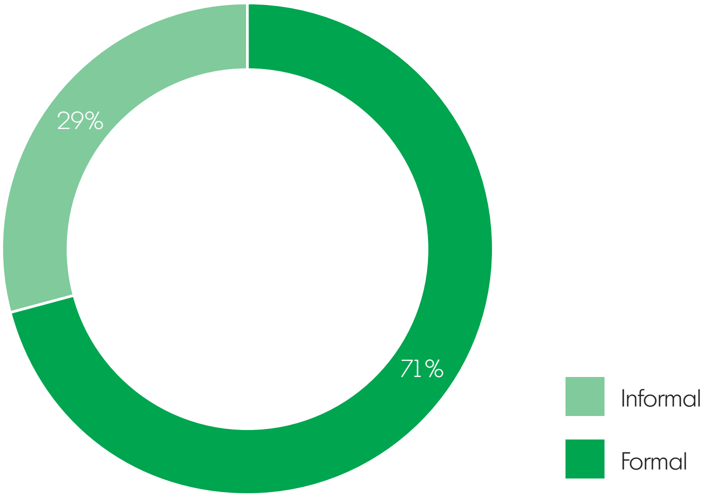
N/g CERTs should continue with such agreements and ensure that the agreements evolve over time to be able to address the ever-changing nature of security threats and vulnerabilities.

Law enforcement

As most n/g CERTs are limited in terms of enforcement authority, they are reliant on law enforcement authorities to respond to clear breaches and violations of the law. The activities of n/g CERTs and LEAs are becoming increasingly intertwined, which is also reflected in a relatively high level of formalised cooperation (see Figure 5).[23] There are two main reasons for this. As part of an n/g CERT's regular monitoring and incident handling activities they can identify network assets, such as command-and-control servers that are part of a botnet, as an example, that are involved in cybercrime activity. In so doing, they can share valuable information with the police, which the police may not have had access to otherwise. Additionally, police officers can uncover useful information during an investigation that would be relevant for an n/g CERT's incident handling and monitoring services. In this context, both organisations share synergies that are mutually beneficial.

Figure 5:
Form of cooperation between n/g CERTs and LEAs

Of what nature is the cooperation between the CERT and law enforcement agencies?



n=17 n/g CERTs

The relationship can become strained, however, depending on local laws regarding data privacy and laws regarding police investigations. In some countries, a police agency may be forbidden, in law or as a policy, from divulging information during criminal investigations. Consequently, information that is useful for an n/g CERT may become outdated by the time the investigation is closed. Nonetheless, overall n/g CERTs report a positive relationship with LEAs and are actively engaging in cooperation with LEAs. LEAs can also benefit from the exchange of technical expertise and knowledge that n/g CERTs can offer.

With few exceptions, relationships between n/g CERTs and law enforcement authorities are based on written agreements. This is widespread throughout the EU. As most n/g CERTs do not have enforcement powers they must turn to relevant law enforcement officials when a clear violation of existing laws is identified. N/g CERTs report good relations with law enforcement authorities.

[23] ENISA covers this topic in more detail in the report 'Cooperation between CERTs and Law Enforcement Agencies in the fight against cyber-crime – A first collection of practices'. (http://www.enisa.europa.eu/activities/cert/support/supporting-fight-against-cybercrime). Also, as part of its work programme 2012, ENISA is investigating the legal and operational barriers and incentives for cooperation between CERTs and other communities, specifically LEAs.

8.2 Cross-Border Cooperation

Due to the distributed nature of cyber-attacks, sometimes managed with infrastructure based in multiple countries and targeting networks across multiple countries simultaneously, the need for international cooperation between n/g CERTs has become more critical. Cyber criminals are often adept at utilising servers and infrastructure in multiple countries to ensure redundancy in their systems. Taking down such operations requires a response that is coordinated geographically and potentially synchronised simultaneously. Otherwise the handling of certain incidents may prove ineffective. To enable such coordinated and timely responses, each country requires a central point of contact that other CERTs know they can reach out to, when needed. N/g CERTs are best positioned to fulfil this role.

"I worry about international cooperation becoming less open and flexible. The international network of CERTs that grew out of the academic world in the 1990s was flexible, decentralised and open. In recent years, as countries have made cyber-security a matter of national security, they have focused capability development in military and intelligence organisations, complicating international cooperation instead of encouraging it."

Statement by an n/g CERT

Keeping up with the increasingly sophisticated nature of cyber threats is also a challenge that all CERTs are facing. Cyber-criminals tend to be well networked and have the ability to exchange expertise. N/g CERTs must also be able to benefit from sharing of knowledge and experiences in order to keep up. A lesson learned and applied in one country is less valuable if it cannot be shared with other CERTs. Forums for sharing best practices and expertise internationally should be considered fundamental to any effective cyber-security strategy. For this reason, initiatives that bring together CERTs provide a critical service to national and international cyber-security efforts. Participation in cross-border initiatives is widespread and overall n/g CERTs speak positively of the value of such organisations. Nonetheless, there is demand for such organisations to focus more or practical exercises and training. N/g CERTs should make an effort to offer practical workshops and exercises during international conferences organised by international CERT and security initiatives. Simulated exercises emphasising actionable skills would make such workshops more useful.

8.2 Cross-Border Cooperation

8.2.1 Gaps and recommendations

Policymakers have embraced cyber-security as a matter of national interest. It is crucial that they focus on real issues of immediate concern.

Gap:

Policymakers across the region need to develop a focused approach to cyber-security as a whole in order to address issues of immediate concern, which may not be the case universally. This is an important issue in the context of allocating resources. Without a focused approach that addresses the most immediate concerns of cyber-security (nationally and internationally), resources, skills and expertise could be misallocated.

Recommendations:

These are ongoing recommendations, which will depend on how 'enlightened' the government is regarding cyber-security issues and cyber-security structures at the governmental level set up in line with national cyber-security strategies.

- The role of the n/g CERTs should be to provide expertise and knowledge on identifying the **technical threats and vulnerabilities to ICT infrastructure** within their respective national borders, as well as providing insight into the abilities of stakeholders (hackers, botnets, etc.) that are actively threatening cyber-security domestically and internationally. They need to communicate this to policymakers and prioritise these threats in the order of the most immediate concerns.

- Policymakers should also take into account feedback from other stakeholders, such as NRAs, who might have a different view of matters related to network security and might be able to share with policymakers relevant indicators that would not otherwise be communicated.

- Dialogue on identifying and prioritising threats and agreeing on the necessary policy responses needs to be done domestically and internationally, due to the fact that cyber-security threats are distributive and cross-border by nature. CIIP operators should be actively engaged in this dialogue because threats can be launched against their infrastructure, or their infrastructure can be exploited.

Gap:

Although the international initiatives are still seen as very valuable for n/g CERTs and welcomed, more value could be added to them by providing a platform for more technical information and practical exercises.

Recommendations:

These are ongoing recommendations and there should be no barriers to implementation provided that the n/g CERTs continue to take an active role in the CERT community/initiatives.

- N/g CERTs should take the initiative to join CERT organisations and contribute to **joint exercises and workshops on sharing expertise.** They should ensure that if they participate in such groups, they take the initiative in helping to organise events and providing feedback and guidance on agendas for events. The n/g CERTs should also encourage voluntary participation of relevant stakeholders including service providers and network operators in cyber exercises and workshops.
- If such organisations do not already exist in various sectors, n/g CERTs should take the initiative by reaching out to relevant stakeholders in the industry and organise ad hoc meetings until a more formal structure can be arranged.
- There remains a high demand from such organisations for the sharing of practical technical expertise. N/g CERTs should ensure that their technical staff have time and resources to maintain regular contact with international organisations and participate in events and information sharing through the organisations. It should be a responsibility of technical staff to actively engage in such organisations and find ways to add value.
- Respective decision-makers should understand the importance of such regular contacts among n/g CERTs and make resources available for these purposes.

8.2.2 Situation overview

Initiatives in cooperation

There are a number of organisations that organise international forums to facilitate cooperation among CERTs and security experts. Such organisations are active in Europe and elsewhere. On a European level, key organisations are TF-CSIRT, Trusted Introducer (TI), EGC[24] and ENISA. On a more global scale, FIRST or the Anti-Phishing Working Group (APWG) are among the more popular organisations. Additionally, there are a number of sector working groups working to facilitate much-needed international cooperation. Still, such organisations face numerous challenges. First and foremost is the issue of trust. Domestic CERTs often have established long-term relationships, due to the fact that security experts often know each other from schools, previous work experience and through local security organisations. The network is less connected outside of countries and regions. Consequently there may be concerns about sharing information in international forums among experts and groups that do not yet have stronger ties. Nonetheless, the ability to network and meet peers is often cited as the most valuable advantage of such organisations. Beyond this, there is demand for organisations to add more value by creating a forum for exchanging more hands-on, practical expertise and best practices. Workshops, joint exercises and deep-dive technology seminars are very much in demand by n/g CERTs.

[24] http://www.egc-group.org/

8.3

Best Practices for Cooperation

Trust

Umbrella initiatives that bring together CERTs and other relevant security bodies can be a useful tool for fostering an environment of trust. They can act as a neutral third party and hasten cooperation that would otherwise require longer-term relationship-building on a bilateral level. The objective of such organisations needs to be defined with a clear goal in mind, specifically the exchange of information and expertise to ensure the ability of security authorities to respond rapidly and in a synchronised manner to address large-scale distributed security vulnerabilities, threats and attacks.

"It's all about trust. If you want to share something, you can always find a way."

Statement by an n/g CERT

Such organisations can coordinate with relevant stakeholders to develop processes and standards for registration and accreditation of security bodies and protocols. Without such procedures, cooperation across borders would ultimately be limited. Beyond serving as a platform for fostering trust, such initiatives can support the CERT community in other ways. By developing standard registration and accreditation criteria, such organisations would provide an additional function of addressing potential skills gaps that may emerge regionally or within specific countries. In order to be registered and receive accreditation, members would have to fulfil criteria deemed necessary by the organisation to achieve a base level of skills that would be relevant for addressing current levels of security threats. Maintaining a common set of skills would also help foster a more trusting environment, as it can be difficult for n/g CERTs with varying skill levels to communicate effectively or feel the need to cooperate with other organisations that have a lower level of expertise. N/g CERTs indicated that they are less open to trusting other organisations that do not share the same level of expertise.

8.3 Best Practices for Cooperation

8.3.1 Gaps and recommendations

Establishing trust remains an ongoing challenge for all n/g CERTs across Europe. There are a number of steps, however, which n/g CERTs and stakeholders can take domestically and internationally to boost trust.

Gap:

An obvious observation is that trust is difficult to build and even more difficult to maintain.

Recommendations:

These are ongoing recommendations. Implementation depends on a high level of cooperation on both national and international level via several means of communication, including most importantly in person.

- Cooperation between n/g CERTs and CII operators can often be best facilitated through mutual, written agreements that are entered into voluntarily. N/g CERTs should continue to engage in such agreements, making sure to review the agreements regularly to adapt to changing security needs and conditions.
- N/g CERTs in multiple countries are engaging in cross-border exercises and training.[25] Such cooperation is valued by n/g CERTs and will likely continue. Participation in international workshops is also commonplace and serves as a useful forum for building contacts and fostering long-term relationships.
- Associations that bring together n/g CERTs should be used to identify skills gaps across the region. **Skills gaps act as an inhibitor to a deeper relationship.** By identifying key skills that are relevant for incident handling and responses, organisations should make an effort to identify where skills are lacking and address the gap through workshops and other forms of expertise exchange.
- Trust can be enhanced among n/g CERTs when they engage, for example, in automated exchange of data or common operational cyber exercises, so that all partners have the feeling of getting 'something in return'.

[25] ENISA is supporting Member States and their n/g CERTs by organising thematic workshops (http://www.enisa.europa.eu/activities/cert/events) and cyber exercises (http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation).

8.3 Best Practices for Cooperation

Gap:

Efforts to standardise information and statistics usually fall short of expectations.

Recommendations:

These are ongoing recommendations. Implementation will depend on the willingness of individual n/g CERTs to abandon their schemes.

- The n/g CERTs should set the right expectations and limit the standards to specific areas while leaving other areas more flexible. Standardised forms for specific information could be a good start. But security needs and technologies are evolving too quickly for any standardisation to be easily manageable or feasible at all. So efforts should be limited with this in mind. The effort should be centralised by an organisation with trusted status and sufficient access to relevant stakeholders.
- N/g CERTs should aim to use recognised standards for exchange of information and naming schemes when available. Of course this will be dependent on resources available and the maturity of the team. Consequently a phased approach would be a useful option.
- Overall, n/g CERTs are implementing relevant security measures to ensure confidentiality and authenticity. Efforts should be made to assure constituents that sufficient security measures are in place.

Gap:

The n/g CERTs have reached different levels of maturity, which may be detrimental to more effective cooperation.

Recommendations:

This is rather a short-term recommendation. Its implementation will depend on budgetary resources, mandate from the government as well as attainment of full membership in CERT initiatives. Based on the interaction with n/g CERTs, reaching one step higher on the maturity level usually takes one year for the n/g CERTs.

- N/g CERTs should make every effort to advance to higher levels on the Maturity Index. Common maturity levels will facilitate greater effectiveness and sustainability locally and facilitate more effective international cooperation.

Gap:

There are differences in terminology and schemes applied by n/g CERTs.

Recommendations:

This is an ongoing recommendation. Its implementation will depend on the willingness of n/g CERTs to abandon their schemes in favour of a common denominator.

- International standards should focus on basic exchange formats, basic taxonomies and classification schemes that can be agreed to in a limited fashion. Efforts for a wide-scale implementation of standards would require tremendous resources and organisation.

8.3.2 Situation overview

Quality of information

The flow of information and, more specifically, the quality, relevancy and consistency of information, is considered to be a key element in developing lasting relationships among n/g CERTs and facilitating coordinated responses. The ability to act in a coordinated manner requires the availability of relevant and accurate data that can be referenced and benchmarked appropriately. Coordination can fall apart if one stakeholder in a group cannot be relied on to provide information that is necessary to ensure effective synchronised responses. There are a number of criteria that need to be considered when trying to ensure a high quality of information:

- **Definitions** – It is important for information to be cross-referenced and benchmarked. For this reason definitions need to be agreed so that stakeholders know what information to include or exclude. Otherwise stakeholders can be comparing two different data sets even though they think they are comparing like with like.
- **Relevancy** – Relevancy is a critical factor in enabling the effective management of data and information sharing. While some n/g CERTs might benefit from access to a great deal of data from their constituents, sharing information that is not relevant makes it more difficult for their counterparts to manage. It is widely reported that a large portion of information exchanged between n/g CERTs goes unused. One factor in this is the irrelevancy of some information but also the inability to sort out what data are relevant and what are not.
- **Timeliness** – To ensure timeliness of data, operators need to agree on schedules for reporting. With appropriate schedules, n/g CERTs can implement necessary measures in advance to ensure schedules are met and, as a result, data are shared at an appropriate time.
- **Context** – Appropriately measured responses to incidents are closely tied to the context of a given threat. While the attributes of one threat might be similar to that of another threat, the potential risks might vary. Putting a threat within agreed contexts can better guide a more targeted response and hasten the decision to alert relevant authorities. Contexts can relate to the origin and target of a threat; namely, is the threat directed at national security, is the threat coming from a terrorist source or an organised criminal network, is there a threat posed by an event of nature and others?

N/g CERTs have expressed the need for standardised definitions. But they also recognise the difficulties in achieving this. Expectations are not high that such a standardisation will be possible, at least on an exhaustive level that addresses all relevant terminology. Incidents are often normalised with a reference number to ensure anonymity. To ensure the security of information, n/g CERTs must implement security measures that ensure the confidentiality, integrity, availability and authenticity of information. N/g CERTs are thorough in implementing necessary security technologies for communications and other schemes to ensure confidentiality. Use of PGP encryption is widespread among n/g CERTs as well as among other CERTs. In many cases n/g CERTs must comply with national laws regarding processing of classified information and implement relevant technologies and systems to comply.

Sustainable reaction

Ensuring sustained incident response and handling capabilities domestically requires an n/g CERT to effectively implement to its full potential all of its service and operational capabilities in a coordinated manner. This requires a sufficiently staffed and managed operation. It also requires a clear mandate that outlines given authorities and clearly defined relationships with relevant stakeholders within the constituency. Ensuring a sustained response as part of an international effort, however, can be far more complicated as more stakeholders become involved. While each individual n/g CERT must still coordinate and implement its services and operational capabilities domestically, ensuring that all participating n/g CERTs are working to their full capacity at the same time depends on the resources and goodwill of each individual n/g CERT and the nature of their relationships with one another. This represents a particular challenge because the skills and maturity level and resources of each n/g CERT vary across Europe. To ensure sustainable cooperation it is consequently important for expectations to be aligned. N/g CERTs should not be in a position to expect a particular response or action from another n/g CERT only to be surprised or unaware that the other n/g CERT does not have the mandate or resources to respond. The Maturity Model can be a useful tool in helping n/g CERTs identify the abilities of other n/g CERTs in advance and adjust their expectations accordingly.[26] This way, if it is known in advance that one CERT is not able to respond in a particular way, the other CERTs can adjust their responses accordingly.

Common terminology and schemes

N/g CERTs report that a high share of information that is available and exchanged often goes unused. There are a number of reasons for this, including the limited availability of resources to manage the information which in part is due to the sheer quantity and frequency of information being transmitted. While this will always be a challenge to manage, one important factor that can ease management of information would be the use of common terminology and schemes. Standardising terminology and schemes is an ongoing challenge. Many attempts go unfulfilled.

For this reason it is important to set the right expectations and try to ensure that standardisation frameworks are flexible enough to keep apace of changing conditions and innovations. At a basic level, certain forms, procedures, classification schemes and taxonomies can be agreed to. But in order for such agreements to be sustainable sufficient management resources must be dedicated to finding the right balance between identifying information that can and cannot fit within a standardisation scheme.

[26] For details on maturity index of n/g CERTs see Annex B of 'Baseline Capabilities of National/governmental CERT – Policy Recommendations', ENISA, 2010.

9

Conclusion

9 Conclusion

N/g CERTs, which play a key role in protecting critical information infrastructure, have now been established in practically all EU Member States. Member States have equipped them with sufficient capabilities in line with recommendations issued by ENISA in 2009 and 2010. The original recommendations on baseline capabilities remain viable also for the current environment. At the same time, some of the original recommendations have not been met to a satisfactory level. Besides, new issues have come up and need to be addressed by n/g CERTs, Member States, CERT initiatives and other stakeholders. The gaps identified and addressed by the updated and new recommendations are mainly legal and political.

There are a number of actions that need to be taken by policymakers in the Member States to support n/g CERTs in their work, especially regarding protection of critical information infrastructure and coordination of incident handling. This requires mandate clarification, as well as incorporating the provisions on n/g CERT into national cyber-security strategies. More concretely, the n/g CERTs should be in a better position to require exchange of information with telecommunication operators/ISPs and law enforcement authorities.

Although the n/g CERTs cannot influence many of the above-mentioned items on their own, other recommendations are well suited to them, too. For example, in a time of economic crisis and with a perceived lack of funding for their activities, n/g CERTs should actively look for additional resources such as EU funds, consulting engagements with the private sector, and research projects. It is also crucial that they add more transparency and visibility by publishing general statistics on incidents and other activities or raising awareness of their actions among their constituency. For this purpose, more focus on PR issues is suggested.

Many of the gaps identified have to be handled by means of cooperation on national and regional level. Cross-border coordination activities performed by ENISA or other CERT initiatives would be desirable, as would the development of a standardised approach to information exchange among n/g CERTs. On the other hand, n/g CERTs should liaise with the private sector in organising accessible and more affordable technical training. The private companies could also take on the job of technology watch from n/g CERTs, so that they can focus on their core services.

This document will be useful for n/g CERTs and policymakers and other stakeholders in the area of cyber-security at national and European level. It should be considered as a living document that will undergo periodic reviews based on the constant evolution of cyber-security and information technology in general. Also, the presented baseline capabilities have to be looked at as a common denominator rather than a one-size-fits-all guide that has to be strictly followed.

10

Annexes

Annex I: Glossary

Artifact handling

An artifact is any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures. Artifacts can include but are not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits. Artifact handling involves receiving information about and copies of artifacts that are used in intruder attacks, reconnaissance, and other unauthorised or disruptive activities. Once received, the artifact is reviewed. This includes analysing the nature, operating principles, version, and use of the artifacts; and developing (or suggesting) response strategies for detecting, removing, and defending against these artifacts. Examples include artifact analysis, response and handling.

Source: www.cert.org/csirts/services.html

'De facto' national CERT

A de facto national CERT acts as a PoC in countries where no official national CERT has as yet been established by the government. Usually the first CERT established in a country is perceived as the de facto national CERT by teams in other countries. De facto national CERTs are indispensable for the management of cross-border incidents until an official national CERT is established or the de facto national CERT is officially mandated by its government.

Source: Baseline Capabilities of National/governmental CERTs

CERT/CSIRT

A Computer Emergency Response Team (CERT) is a team of IT security experts whose main business is to respond to computer security incidents. The team provides the necessary services to handle them and support their constituents to recover from computer security breaches. In order to mitigate risks and minimise the number of required responses, most CERTs also provide preventative and educational services for their constituency. The constituency (an established term for the customer base) of a CERT usually belongs to a specific sector, such as academia, companies, governments or military. The term CSIRT (Computer Security Incident Response Team) is a more modern synonym and should reflect the fact that CERTs developed over time from being mere reaction forces towards more universal providers of security services.

Source: Baseline Capabilities of National/governmental CERTs

Critical Information Infrastructure (CII)

ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.). Critical infrastructures are those systems that provide the resources upon which all functions of society depend. Examples are (apart from telecommunications) transportation, energy, water supply, health care, emergency services, manufacturing and financial services.

Source: Green Paper on a European Programme for Critical Infrastructure Protection COM(2005) 576 final and other sources

CSIRT *see* CERT

Governmental CERT

Informal definition: a CERT that is responsible for the protection of governmental/administrative networks. The constituency of a governmental CERT therefore is the government and other public bodies. In many cases a governmental CERT also acts as national CERT. Definitions may vary across the EU Member States.

Source: Baseline Capabilities of National/governmental CERTs

National CERT

Informal definition: a CERT that acts as national point of contact (PoC) for information sharing (like incident reports, vulnerability information and other) with other national CERTs in the EU Member States and worldwide. National CERTs can be considered as 'CERT of last resort', which is just another definition of a unique national PoC with a coordinating role. In many cases a national CERT also acts as governmental CERT, although definitions may vary across the EU Member States.

Source: Baseline Capabilities of National/governmental CERTs.

Annex I: Glossary

National/governmental CERT (n/g CERT)

The informal definitions for 'national CERT' and for 'governmental CERT' do not uniquely reflect the status, role and responsibility of all the CERT teams ENISA tries to address. In the context of this document and ENISA's work in the area of baseline capabilities the term 'national/governmental CERT' (n/g CERT) has been introduced. This term subsumes all the types of national, governmental, national points of contact, etc., in the Member States, which are:

- generally supporting the management of security incidents for systems and networks within their country's borders;
- bearing responsibilities for critical information infrastructure protection (CIIP) in its country;
- acting as official national point of contact for n/g CERTs in other Member States.

The term 'national/governmental CERT' therefore subsumes all 'flavours' of national CERTs, governmental CERTs, national points of contacts and others in the EU Member States.

Source: Baseline Capabilities of National/governmental CERTs

Proactive services

Proactive services are designed to improve the infrastructure and security processes of the constituency before any incident or event occurs or is detected. The main goals are to avoid incidents and to reduce their impact and scope when they do occur. Examples of proactive services include announcements, audits, maintenance/development of security, intrusion detection, and information dissemination.

Source: www.cert.org/csirts/services.html

Reactive services

Reactive services refer to services that are designed to respond to requests for assistance, reports of incidents from the CSIRT constituency, and any threats or attacks against CSIRT systems. Some services may be initiated by third party notification or by viewing monitoring or IDS logs and alerts. Examples of reactive services include incident handling/analysis, vulnerability handling/analysis and forensic evidence collection.

Source: www.cert.org/csirts/services.html

Security Quality Management Services

Services that fall into this category are not unique to incident handling or CSIRTs in particular. They are well-known, established services designed to improve the overall security of an organisation. By leveraging the experiences gained in providing the reactive and proactive services described above, a CSIRT can bring unique perspectives to these quality management services that might not otherwise be available. These services are designed to incorporate feedback and lessons learned based on knowledge gained by responding to incidents, vulnerabilities and attacks. Feeding such experiences into the established traditional services (described below) as part of a security quality management process can improve the long-term security efforts in an organisation. Depending on organisational structures and responsibilities, a CSIRT may provide these services or participate as part of a larger organisational team effort. Examples include risk analysis, business continuity and disaster recovery planning, testing plans (local and inter-operational manoeuvres) and testing methodology, security consulting, awareness building, education/training, vulnerability assessment/management, product evaluation/certification.

Source: www.cert.org/csirts/services.html

Annex II: Abbreviations

APWG	Anti-Phishing Working Group
BCM	Business Continuity Management
CERT	Computer Emergency Response Team
CERT/CC	CERT Coordination Centre
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CSIRT	Computer Security Incident Response Team
DRP	Disaster Recovery Planning
EC	European Commission
EFTA	European Free Trade Association (Iceland, Liechtenstein, Norway and Switzerland)
EGC	European Government CERTs
ENISA	European Network and Information Security Agency
EU	European Union
FIRST	Forum of Incident Response and Security Teams
FTE	Full-Time Equivalent
FTP	File Transfer Protocol
IMPACT	International Multilateral Partnership Against Cyber Threats
IT	Information Technology
KPI	Key Performance Indicator
LEA	Law Enforcement Authority
NCSS	National Cyber-security Strategies
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NRA	National Regulatory Authority
PGP	Pretty Good Privacy
PoC	Point of Contact
S/MIME	Secure/Multipurpose Internet Mail Extensions
SLA	Service-level agreement
TF-CSIRT	Task Force-CSIRT
TI	Trusted Introducer
VoIP	Voice over Internet Protocol
WP	Work Programmes
WWW	World-Wide Web

Annex III: Web resources

- Websites of National/governmental CERTs and other CERTs in the Members States of the EU and EFTA, https://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe
- Websites of policymakers and other stakeholders in the area of cyber-security strategy in the EU and EFTA Member States
- Document: 'Baseline Capabilities for national/governmental CERTs (operational aspects and policy recommendations)', http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities
- Document: 'Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime – A first collection of practices' (ENISA), http://www.enisa.europa.eu/activities/cert/support/supporting-fight-against-cybercrime
- Document: 'A flair for sharing – encouraging information exchange between CERTs' (ENISA), http://www.enisa.europa.eu/activities/cert/support/legal-information-sharing
- Document: 'CERT operational gaps and overlaps' (ENISA), http://www.enisa.europa.eu/activities/cert/other-work/gaps-overlaps-report
- Document: 'CSIRT set-up guide' (ENISA), http://www.enisa.europa.eu/activities/cert/support/guide
- Document: 'Good Practice Guide on Incident Reporting Mechanisms' (ENISA), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents%20reporting/good-practice-guide-on-incident-reporting/good-practice-guide-on-incident-reporting-1
- Document: 'Good Practice Guide for National Exercises' (ENISA), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/exercises/national-exercise-good-practice-guide
- Document: 'National Cyber-security Strategies' (ENISA), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper
- EU legislation and strategic documents related to information society, cyber-security and especially Critical Information Infrastructure Protection including the document National Cyber-security Strategies (ENISA), http://ec.europa.eu/information_society/policy/nis/index_en.htm
- Strategic Trends 2012: Key Developments in Global Affairs 2012, http://www.css.ethz.ch/publications/pdfs/Strategic-Trends-2012.pdf
- E. Koivunen: 'Effective Information Sharing for Incident Response Coordination', http://personal.inet.fi/koti/erka/Studies/DI/DI_Erka_Koivunen.pdf
- TF CSIRT publications and presentations, http://www.terena.org/publications/
- FIRST publications, http://www.first.org/

Annex IV: Questionnaire for national/ governmental CERTs

Updated Baseline Capabilities for National/Governmental Computer Emergency
Response Teams (CERTs)

Organisation Details

Your Name

Job Title/Position:

Contact details (phone number, email):

Job Description (please indicate your main responsibilities):

Responsibility	Insert an 'x' Next to the Relevant Responsibility
Management	
Technical	
Legal	
Other (please specify)	

How long have you been in this position?:

How long has your team been operating?:

What type of CERT is your organisation (please indicated in the box below)? For detailed definition see the Glossary.

Type of Organisation	Insert an 'x' Next to the Relevant Category
National	
Governmental	
National/Governmental	
De Facto National	
Other (please specify)	

Note: Please, feel free to attach links to external documents (special laws and regulations, recommendations, standards, etc.) or enclose internal documents (descriptions of processes, procedures, instructions, organisational schemes, cases, etc.) everywhere it is suitable and possible.

Section A: MANDATE FOR NATIONAL/GOVERNMENTAL CERTs

Objective of Section A – Questions in Section A are designed to understand the current status of the national/government CERT's mandate and gather feedback on its effectiveness.

A1. Who/what provides the mandate for your CERT? Please state if there is a strategic document, legislation or other source that defines your mandate. Please identify and describe the specific documents or legislation or other sources.

A2. For how many years is your mandate defined? In other words, when will your mandate expire? On which basis is it renewed (if applicable)?

A3. If there is a mandate for your CERT, are all services that your CERT offers covered by the mandate, or do you offer other services that are outside the mandate? If you offer any services not covered by the mandate, please describe them and specify to which part of the constituency it is provided.

A4. In your opinion, are all roles and responsibilities of the team clearly defined in the current mandate or do you think changes need to be made to clarify the mandate? If yes, please describe them.

A5. Does your mandate include a role in the national cyber-security law/strategy development? This could include, for example, assessment of risks, creation of a risk management plan for CIIP, implementation of the plan, verification of its effectiveness, and regular evaluation and improvement of the CIIP plan. If the role is not specified in the mandate, do you have an informal role in the national cyber-security law/strategy? If yes, please describe.

A6. Is/was your CERT involved in the process of developing the national cyber-security law/strategy?

A7. Is your CERT team hosted in or operated by a 'higher' organisation (cyber-security centre, ministry, regulatory agency, etc)? If yes, please identify and describe that organisation. Is there a special law that defines the relationship between your team and the host organisation, or are there just arrangements within the host organisation (internal agreement or policy)?

A8. Is your host organisation responsible for the national cyber-security agenda in your country (including crisis situation and the CII protection)?

A9. In your opinion, how should the mandate of the national/governmental CERT in your country be strengthened to improve its contribution to protecting national cyber-security and critical information infrastructure in particular? Please give one or several ideas.

A10. Is there any new legislation currently being developed that would impact your CERT's mandate? If yes, please describe. Are you actively involved in developing the new legislation or is your feedback being considered in any way?

A11. In case of a cyber-security crisis (e.g. large scale cyber attack) does your team or your host organisation have in place a direct line of accountability to an appropriate section within the national executives? Is it officially formalised (document, policy, agreement, etc.)? Please explain.

A12. Is your team involved in the risk management process regarding the national critical information infrastructure protection? If yes, what is your specific role?

A13. Is your team an official Point of Contact (PoC) for other CERTs (national/governmental CERT included) and with other members of the security community? Is this role formally specified in your mandate? How does this single contact point role work in day-to-day operations? Please describe both positive and negative remarks and suggestions for improvement.

Section B: SERVICE PORTFOLIO OF NATIONAL/GOVERNMENTAL CERTS

Objective of Section B – Questions in Section B are designed to understand and identify the services provided to your constituencies.

B1. Please describe your constituency (ies).

B2. Please list all the services that you provide for the relevant constituencies according to the relevant service categories. It is important that you list all the services within each of the listed categories. Please refer to the Glossary for service definitions.

Constituencies	Proactive Services	Reactive Services	Artifact Handling	Security Quality Management Services	Other Services
Government and Public Bodies					
Critical Information Infrastructure Organisations					
Other Domestic CERTs					
End Users					
Other Stakeholders Within the State's Border (specify)					
Other					

B3. Are there any other services that your team provides and which are considered 'new' within the typical CERT services portfolio (see the Glossary for the identification of the typical CERT service portfolio)? If yes, please describe them and indicate to which part of the constituency you provide them?

B4. Are there any services that you outsource to third parties? If yes, which ones and how long have you been outsourcing? Are you satisfied with outsourcing these services? If not, please specify which service and why. How do you outsource these services (e.g. following tender procedures, etc.)? Do you plan to outsource any services in the future that are currently handled internally? If yes, describe which services, why and when.

B5. Is your team actively involved in business continuity management and disaster recovery planning for national critical information infrastructure protection? Please describe your active role.

B6. Does your team provide your constituents with more advanced education and training on best practices in cyber-security (e.g. by organising national cyber-security exercises involving key constituents like CII)? If yes, how often?

B7. In your opinion does the CERT service portfolio table (see the table in the Glossary) still reflect the actual services provided by CERTs? Which services should be added or deleted concerning the national and governmental CERT? (e.g. cybercrime related services, legal aspect of services, PR services, etc.) Please describe and explain.

Section C:
OPERATIONAL CAPABILITIES OF NATIONAL/GOVERNMENTAL CERTS

Objective of Section C – Questions in Section C are designed to gather feedback on your team's internal operations (operational capabilities).

C1. Please describe the maturity status of your team. Please indicate (in the table below) the phase in which your team is currently found (for details see the National/Governmental CERT Maturity Model in the Glossary).

Status	Insert an 'x' Next to the Relevant Status
Initial	
Repeatable	
Defined	
Managed	
Optimised	
Other (please specify)	

C2. Please describe your team's funding model. Do you consider that the allocated resources are sufficient concerning the scope of your work (responsibilities and roles) formally defined for your team? Please elaborate.

C3. Please indicate the current size of your staff, providing details on the number of full-time and part-time staff. Do you plan to increase or decrease the number in the coming year(s)? If yes why, by how much, and when?

C4. Please provide details on the composition and types of responsibilities allocated to your team, for example: team leader (manager, coordinator), incident handlers, technical expert, support staff, legal, other? Please identify the responsibilities and number of staff for the various responsibilities.

C5. In your opinion what is the missing capability within your team concerning the specific human resources skills (specific technical, legal, PR or other skills)? Why?

C6. For each of the services outlined in Section B, indicate the number of staff that is allocated and identify the responsibilities (team leader, managerial, technical, legal, etc.)?

Service	Number of Staff	Responsibilities
Proactive Services		
Reactive Services		
Artifact Handling		
Security Quality Management Services		
Other Services		

C7. Please provide details on your office hours? Are your services available 24/7/365? If not, indicate when they are available and if some services are available during different hours than other services. In case of emergency, is your staff available out of working hours? If yes, please specify the number of people and their roles. Are some of your staff members available for on-call services or available during shifts?

C8. Do you inform your constituency of how they can contact you? Please explain how do you do that for all types of your constituency and services provided.

C9. Please describe the physical security measures that are currently being used to safeguard the premises. Also describe what physical security measures are provided, if any, for visitors that may be different than the day-to-day measures used to safeguard the premises.

C10. Please describe which tools are available for constituents or other outside parties (e.g. other national/governmental CERTs, national executives, outsource companies, if any) to communicate with you (telephone, email, website, etc.). To what extent are these tools backed up or made resilient to ensure that communications channels do not fail?

C11. What level of security is implemented to ensure privacy and security of electronic communications (please indicate if you use encryption, the type of encryption, etc.)? Please indicate if different measures are used to ensure internal communication, communication with external bodies (other national/governmental CERTs, national executives, outsourced companies, if any), and communications of visitors that might be present onsite temporarily.

C12. How does your CERT secure that the information disseminated to stakeholders is relevant, complete and comprehensible? What information quality standards has your CERT defined, such as exchange and naming schemes?

C13. Does your team or the host organisation have any service management and quality systems/ processes that are designed to follow-up on performance and improve performance? If yes, please describe. If not, do you plan to implement any systems/processes and when? Please describe what you plan to implement.

C14. Which sources of information for good practices, if any, do you employ for incident reporting forms, information classification schemes, procedures to handle critical incidents and the issues of priority and feedback? Such sources for good practices may include your internal national practices, ENISA reports, ITU reports, SCAP (Security Content Automation Protocol) standards and others.

C15. Does your CERT have a role in disseminating or defining terminology and definitions for use within the national cyber-security community and CIIP stakeholders domestically?

C16. How do you train your staff? Do you organise internal training for new staff? Does your staff attend training such as TRANSIT Training, etc.?

C17. In your opinion, are there enough opportunities for training for your staff (internal, national, European, International)? Please elaborate, in all cases, the possible shortcomings and how to overcome them?

Section D: NATIONAL AND CROSS-BORDER COOPERATION

Objective of Section D – Questions in Section D are designed to understand current cooperation models between the national/government CERTs in Europe and with other stakeholders mainly within the national and regional scope.

Section D, Part 1 – Cooperation Between National/Governmental CERTS in Europe

D1. What international CERT structures and initiatives (TF-CSIRT, Trusted Introducer – TI, ENISA initiatives, FIRST, European Government CERTs Group etc.) are you a member of? Which of these organisations do you consider as the most beneficial for the functioning for your CERT and why?

D2. Has your CERT engaged in any formal or informal bilateral partnership with national / governmental CERTs in other EU Member States? Please specify. Please describe also the legal models and advantages/disadvantages of the cooperation.

D3. Which means does your team use for cooperation with national/governmental CERTs in Europe (personal visits, meetings within CERT associations or conferences sessions, videoconferences, phone calls, e-mail exchanges, other means)?

D4. Which members of your team, and of the team of your cooperating national/governmental CERT partner, are involved in such cooperation (team leaders, chief incident handlers, technical experts, legal experts)?

D5. In your opinion, what characteristics should the national/governmental CERT possess in order to be considered trustful (i.e. being able to exchange real incident data, etc.) by other CERTs in Europe or by the wider cyber-security community?

D6. Is your cooperation with national/governmental CERTs in other EU Member States based rather on the synergy effects of regional cooperation or on the maturity stage of the cooperating national/governmental CERT? See Glossary for more details.

Section D, Part 2 – National and Regional Cooperation with Other Security and CIIP Stakeholders

D7. Can your team require its constituents to implement measures to counter cyber-security threats or is the cooperation based on a voluntary model? Is there a formal framework that outlines your CERT's authority over its constituents? Please describe.

D8. If your constituents consist of (critical information) infrastructure operators and Internet service providers, what is the framework of your cooperation (written agreements, legislation, informal agreement, etc.) and how frequent is the communication?

D9. What is the framework for cooperation (written agreements, legislation, informal agreement, etc.) between your CERT and national and international law enforcement authorities? Please identify the type of law enforcement authorities you cooperate with domestically and internationally (if relevant).

D10. Is there a formal procedure for cooperation between your team and other domestic CERTs such as an association/community of CERTs or a working group? Could you briefly describe strengths and weaknesses of this cooperation? What kind of information is exchanged as part of this cooperation? How often does this community or group meet? What is the role of your team within these meetings?

D11. Which national stakeholders (public, governmental, private, industry, academic, etc.) are the regular members of this community or working group? In your opinion, which parties are still missing from this group and why? What are the obstacles to their cooperation? How should the obstacles be overcome in your opinion?

D12. As a team who has a leading role in incident handling within the national borders, what do you consider as the main obstacle to a smooth cooperation (concerning regular and ad hoc information and data exchange and support) between cyber-security stakeholders on a national level and what should be done to improve the situation?

D13. Should there be any different requirements for specific constituents such as CIIP companies and bodies? Why? Please elaborate.

Section E: Additional Feedback

E1. In your opinion are the currently defined baseline capabilities of national/governmental CERTs sufficient or do you think they should be changed? If so, in which areas and why?

E2. In your opinion what are the main obstacles that the national/governmental CERTs face and how could these obstacles be mitigated?

E3. If there are any other comments you have, or feedback, please feel free to write them here.

Thank you for your time.

Annex V: Questionnaire for other stakeholders (other than national/governmental CERTs)

Updated Baseline Capabilities for National/Governmental Computer Emergency Response Teams (CERTs)

Organisation Details

Your Name:

Contact Details (job position, phone number, email):

Job Description (please indicate your main responsibilities):

Responsibility	Insert an 'x' Next to the Relevant Responsibility
Management	
Technical	
Legal	
Other (please specify)	

How long have you been in this position?:

What is the name of your organisation?:

What is the type of your organisation (please indicate in the table below)?:

Type of Your Organisation	Insert an 'x' Next to the Relevant Type
CERT	
Policymaker (ministry)	
Regulator	
Cyber-security centre and other government agency dealing with cyber-security	
Critical Information Infrastructure Operator	
Other operator and service provider	
Vendor	
Independent expert	
Other (please specify)	

If you identified your organisation as a CERT in the previous table, please indicate the type of your constituency in the table below (Otherwise, skip the table and proceed further in the questionnaire):

Annex V: Questionnaire for other stakeholders (other than national/governmental CERTs)

CERT Type	Insert an 'x' Next to Each Relevant Constituency
Academic Sector	
Commercial	
CIP/CIIP Sector	
Governmental Sector	
Internal	
Military Sector	
National	
Small & Medium Enterprises (SME) Sector	
Vendor	
Other (please specify)	

Note: Please, feel free to attach links to external documents (special laws and regulations, recommendations, standards, etc.) or enclose internal documents (descriptions of processes, procedures, instructions, organisational schemes, cases, etc.) everywhere it is suitable and possible.

Please try to answer all the questions or as many of them as possible. It may happen that a few questions will not be relevant for your organisation, you will not be sufficiently knowledgeable of the topic or for some other reason you will not be able to answer them. In this case you can indicate that the question(s) is (are) not relevant for your organisation or skip it (them) and proceed to the next question.

Section A: MANDATE FOR CERTs

Objective of Section A – Questions in Section A are designed to understand your organisation's awareness of the national/government CERT and gather feedback on the effectiveness of its mandate.

A1. Which organisation (please give name) acts as the national/governmental CERT in your country?

A2. Please describe your working relationship with the national/governmental CERT in your country. On which legal basis is this cooperation based?

A3. Is the cooperation part of the framework for the national cyber-security strategy or other strategic document? (CIIP strategy, crisis situation management, etc)?

A4. In your opinion, does the current mandate of the national/governmental CERT clearly define the team roles and responsibilities or do you think changes need to be made to clarify it more? If yes, please describe.

A5. In your opinion, how (if necessary) should the mandate of the national/governmental CERT in your country be strengthened to improve its contribution to protecting national cyber-security and critical information infrastructure?

Section B: SERVICE PORTFOLIO OF NATIONAL/GOVENRMENTAL CERTS

Objective of Section B – Questions in Section B are designed to understand and identify the services your organisation receives from the national/government CERT and gather your opinions on their quality and effectiveness.

B1. Please indicate a category of constituency your organisation fits the best:

Category of Constituency	Insert an ‘x’ Next to the Relevant Category
Government and Public Body	
CIIP Organisation	
Other Domestic CERT	
End User	
Other Stakeholder within the State’s Border	
Other (please describe)	

B2. Please list all the services that you receive from the national/governmental CERT according to the relevant service categories. It is important that you list all the services within each of the listed categories. Please refer to the Glossary for service definitions.

Proactive Services	Reactive Services	Artefact Handling	Security Quality Management Services

B3. Are there any other services that do not fit into the above categories that you receive from or provide to the national/governmental CERT?

B4. What is your satisfaction with the services provided by the national/governmental CERT? What is the main benefit for you from these services? Are there services that need improvement? Where, in your opinion, is the biggest potential for improvement?

B5. Are there any other services that the national/governmental CERT should offer to its constituencies in your country? Why? Please elaborate.

B6. If you identified new services in the previous question, which problem would they help to mitigate and what would be the biggest obstacle for implementing these new services?

B7. Are there services provided by the national/governmental CERT which you do not consider to be necessary? Please describe.

Section C:
OPERATIONAL CAPABILITIES OF NATIONAL/GOVERNMENTAL CERTS

Objective of Section C – Questions in Section C are designed to gather feedback from your organisation on the operational capabilities of the national/government CERT and your opinions on their effectiveness.

C1. Are you familiar with the current resources of the national/governmental CERT? If yes, is the current size of staff of the national/governmental CERT sufficient, in your opinion, or do you think it should be increased in order to be able to handle the tasks resulting from its mandate?

C2. Do you think that the composition of the staff of the national/governmental CERT is sufficient in that it balances the need to have a functioning team consisting of a team leader, incident handlers, technical experts and supporting staff? In your opinion, does the national/governmental CERT possess enough expertise to fulfil its roles and responsibilities within the country properly?

C3. Regarding question B1 (which services do you receive from the national/governmental CERT), on what time basis (24/7/365, business hours only, combination of both depending on services offered, etc.) are the services available to your organisation?

C4. Does the national/governmental CERT inform you of how it can be contacted? What are the options that they offer?

C5. Are you aware (from your experience as a visitor to the national/governmental CERT building) of the physical security measures that are currently being used to safeguard the premises of the national/governmental CERT?

C6. What tools (telephone, email, web site, etc.) does your organisation use to communicate with the national/governmental CERT? To what extent are these tools backed up or made resilient to ensure that communications channels do not fail?

C7. What level of security is implemented to ensure privacy and security of electronic communications when contacting the national/governmental CERT (please indicate if you use encryption, the type of encryption, etc.)?

C8. Is the format (including the template for reporting incidents) for communication with the national/governmental CERT sufficient for you or would you recommend changes to improve it further?

C9. If you reported any incident to the national/governmental CERT, can you describe the way the incident was dealt with, especially in regards to communication and feedback from the national/governmental CERT? Were you satisfied with the feedback and approach of the national/governmental CERT when dealing with the incident you reported?

Section D: NATIONAL AND CROSS-BORDER COOPERATION

Objective of Section D – Questions in Section D are designed to understand current cooperation models between the national/government CERT and other stakeholders.

D1. Does the national/governmental CERT require your organisation to implement measures to counter cyber-security threats or is your cooperation based on a voluntary model? Is there a formal framework that outlines your national/governmental CERT's authority over its constituents?

D2. What is the framework (written agreements, legislation, informal agreement, etc.) for your cooperation with the national/governmental CERT?

D3. How frequent is your communication with the national/governmental CERT and what format does it take?

D4. In your opinion, what characteristics should the national/governmental CERT possess in order to be considered trustful (i.e. having a good reputation) by other CERTs in Europe or by the wider cyber-security community? Do you think that the national/governmental CERT in your country can be considered trustful by its constituents?

D5. How would you describe the level of cooperation between your organisation and the national/governmental CERT? Are there any obstacles to a smooth cooperation and if there are, how could they be mitigated in your opinion?

D6. Is your organisation a member of any working group or initiative organised by the national/governmental CERT in your country? If yes, are you satisfied with the format of the meetings? If not, do you plan to initiate a change? Please elaborate.

D7. Which other platforms and initiatives would you mark as the most suitable for national and especially regional cooperation on cyber-security?

D8. Are you aware of any kind of regional cooperation that the national/governmental CERT in your country is taking part of? If so, please specify.

D9. What should the existing platforms and initiatives (TF-CSIRT, FIRST, ENISA etc.) focus on in order to increase international cooperation and exchange of information in the fight against cyber crime?

Section E: Additional Feedback

E1. Are the currently defined baseline capabilities of the national/governmental CERTs sufficient or do you think they should be changed? If so, in which areas and why?

E2. From your perspective, what are the main obstacles that the national/governmental CERTs face and how could these obstacles be mitigated?

Thank you for your time.

Annex VI: Discussion Guide for Interviews

DISCUSSION TOPICS FOR INTERVIEWS WITH N/G CERTS

Note: At the beginning of each interview the questions from this discussion guide were preceded by questions aiming at clarification of responses to the survey. Also, if a question from this discussion guide had been already addressed by in the survey, it was no longer used in the interview.

GENERAL
Do you think that the evolving cyber-security landscape also implies change in the role of the national/governmental CERTs?
In what time horizon do you plan to reach the next phase in the maturity status (in your case repeatable)?

MANDATE & STRATEGY
Does your website include the RFC 2350 document? If this is the case, when was it last updated?

SERVICE PORTFOLIO
What do you consider as the main obstacle in handling incidents internationally? Please elaborate especially on the technical part of this topic?
Is your CERT adequately equipped as regards incident handling in terms of tools and data/information to process? What tools/mechanism do you use for incident handling? Are you satisfied with the chosen tools? (pros and cons)
Would you prefer to have one standardised format to exchange data/information among n/g CERTs only and to discuss this topic with other n/g CERTs?
How often do you release statistics on incidents? Are these statistics made public or not? Do you provide also an English version of the statistics? How do you sort data in these statistics (type of incident, solved/unsolved etc.)?

OPERATIONAL CAPABILITIES
What is your average yearly budget? If you are unable to give the precise figure at least indicate whether the budget is sufficient for fulfilment of all tasks included in the mandate of your CERT or requested from your constituents?
How often do you publish information about threats regarding your constituency? What kind of communication do you use for alerting your constituents? Do you provide this information in English, too?
Many CERTs have identified hiring qualified personnel for incident handling as a problem? How do you motivate IT specialists to work at your organisation? Do you offer competitive salaries and other benefits?

COOPERATION
On what type of incidents do you work under the regional cooperation with other CERTs, ISPs and other partners? Is the cooperation more straightforward on the regional level than it is on the European and global level?
Apart from the current multilateral and bilateral cooperation forms are you in favour of creating another structure, for example association of CERTs in your region?
In what area is the cooperation among n/g CERTs needed and missing? Why?
What are the main sources your organisation employs for learning about best practices in CERT activities? Are these sources international fora like FIRST, TERENA, ENISA initiatives and reports, bilateral meetings, etc.? Is there anything specific (in terms of tools, means, public awareness events) which might help you to improve your team's work?

Annex VII: List of original policy recommendations on Baseline Capabilities

Mandate & Strategy

National cyber-security & CIIP strategy

- Member States should consider adopting a holistic, coordinated national approach to cyber-security and CIIP that is aligned with the European strategy, its policy context and risk management practices. Member States should make sure that all relevant stakeholders are involved in the national approach to these issues and their roles are clearly identified, including the role of the national/governmental CERT.
- National/governmental CERTs should be key components of national cyber-security and critical information infrastructure protection strategy. Consequently, the roles of the national/governmental CERTs should be translated into a formal mandate with detailed specifications of the capabilities required to carry out the mandate.

Mandate – Hosting organisation

- The national/governmental CERT should be mandated in line with the national cyber-security and CIIP strategies. When established within a hosting organisation with broader responsibilities, the host should provide a sufficient, official and legal framework to allow the national/governmental CERT to undertake its responsibilities and perform its roles in full.
- If a de facto national/governmental CERT exists, the government should provide that CERT with an official mandate and consider moving it into a suitable hosting organisation. If neither a de facto nor an officially mandated national/governmental CERT exists, the government should consider creating an officially mandated national/governmental CERT and decide whether it should be located within a hosting organisation.
- The hosting organisation of the national/governmental CERT should be qualified to report on cyber-security matters and should have a direct line of accountability to an appropriate section within the national executive.

Mandate – Constituency

- The constituency of a national/governmental CERT should consist of all domestic stakeholders, ie, the full national domain. However the national/governmental CERT should not provide the full range of its services to the whole of its constituency. Within its constituency, certain groups should be distinguished for the delivery of various parts of its service portfolio. Accordingly, priorities need to be set for:
  - government and public bodies
  - critical Information Infrastructure organisations
  - other stakeholders within the state's borders.

Mandate – Roles and responsibilities for the national/governmental CERT

- When formalising the mandate of a national/governmental CERT, its roles and responsibilities should be adequately and clearly defined and supported by government policy and regulations.
- A national/governmental CERT should be mandated to act as the official national PoC for CERTs (and, where appropriate, other members of the security community) in other countries.
- A national/governmental CERT should be involved in the risk management process regarding the critical information infrastructure protection. The CERT should play an active role in implementing and monitoring the national CIIP strategy and in crisis management situations; e.g., significant security incidents affecting the CII should be reported to the national/governmental CERT and that CERT should have a coordinating role in the resolution of the crisis.

Service Portfolio

Core services

- A national/governmental CERT must minimally provide an effective incident handling capability for its constituents. Handling cyber-security incidents on a national or cross-border scale, and incidents related to critical information infrastructure, should be the absolute priority of a national/governmental CERT.
- A national/governmental CERT should also provide the core proactive services, ie, alerts, warnings, announcements and the dissemination of security-related information. These services aid in reducing the number and severity of cyber-security incidents by providing proactive assistance in securing the constituency's infrastructure. Furthermore, these services can be provided to the entire constituency at one and the same time, so that the effort and cost involved is relatively low compared to the added-value they provide to the constituency.
- At a higher maturity level, and given sufficient staff and resources, a national/governmental CERT can implement other services, preferably based on a risk assessment which identifies the most critical needs of the constituency.
- The national/governmental CERT should be actively involved in business continuity management and disaster recovery planning for national critical information infrastructures. In addition, it should strive to build a capability in dynamic risk analysis (situational awareness) with regards to the country's critical information infrastructures.
- An essential role of the national/governmental CERT should be to build broad public awareness of the risks associated with online activities using public awareness campaigns on cyber-security.
- If resources are available, the national/governmental CERT should also provide its constituents with more advanced education and training on the best practices in cyber-security by, for example, organising national cyber-security exercises involving key constituents (e.g., critical information infrastructure).

Operation

Human resources – Operation mode

- Adequate and appropriate human resources should be dedicated to supporting the operation of the national/governmental CERT. To provide an acceptable level of service (including being reachable 24/7/365 for incident handling), national/governmental CERTs that are just starting up should strive to have a minimum of six to eight FTEs. However, periodic assessments of the appropriate staffing level, based on the size of the constituency and the breadth of services offered, are necessary.

- The human resources that are dedicated to the CERT need to have appropriate skills and expertise, which requires adequate investment. A profile of the staff required would include a team leader, several incident handlers and several technical experts.

Infrastructure

- The national/governmental CERT should ensure high availability of their communications services by avoiding single points of failure and have at least several means for being contacted and for contacting others. Furthermore, the communication channels should be clearly specified and well known to the constituency and cooperative partners.

- Security measures to ensure the confidentiality and integrity of information in transit (secure e-mail, https) and at rest (encryption, access control) should be implemented and managed by the national/governmental CERT.

- The national/governmental CERT should be secure in every way, not only logically but also in the physical sense. The offices and the supporting information systems must be located in secure sites.

Provision of services

- A service management quality system should be created to follow-up on the performance of the national/governmental CERT and ensure a continuous process of improvement. This could be based on clearly defined metrics that include formal service levels and key performance indicators.

- In order to increase the efficiency and effectiveness of the services of the national/governmental CERT, supporting processes and procedures should be defined and supporting tools should be implemented.

Business continuity

- Continuity of the national/governmental CERT should be ensured by:
  - A proper system for managing and routing various requests, in order to facilitate handovers. This system also serves as a knowledge base on a certain report where every collaborator adds his comments and analysis to the document.
  - Full-time staffing of the national/governmental CERT to ensure availability at all times.
  - Ensuring continuity of the infrastructure. Redundant systems and backup working space should be set up for the national/governmental CERT to ensure access to the means of communication in the face of attacks and/or system failures.
  - Hiring adequate staff and making provision for ongoing staff training and exercises.

Cooperation

National cooperation – Constituency

- The authority of a national/governmental CERT over its constituency may be regulated in such a way that the national/governmental CERT can require its constituents to implement measures to counter threats. However, appropriate limits should be placed on the scope of this authority as it also has disadvantages.

National cooperation – Internet service providers / telecommunication network operators

- In line with their mandate, national/governmental CERTs should establish particular cooperative relationships and procedures with internet service providers and telecommunication network operators. These, typically private, companies play a key role in the handling of large-scale incidents and are part of the national critical information infrastructure.

- Where a national internet service providers' or telecommunication network operators' community exists, national/governmental CERTs should consider being involved in the community or in a relevant working group (e.g., a security workgroup). Where such a community or group does not exist, the national/governmental CERT should consider organising a cooperative community with the internet service providers and telecommunication network operators.

National cooperation – Other CII operators

- In line with their mandate, national/governmental CERTs should establish particular cooperative relationships and procedures with all relevant critical infrastructure operators as part of the national CIIP strategy. Where a critical information infrastructure community exists, national/governmental CERTs should be involved in the community or in a relevant working group (eg, an information security or networking workgroup). Where such a community or group does not exists, the national/governmental CERT should consider organising a cooperative workgroup on cyber-security for the operators of critical information infrastructure.

Annex VII: List of original policy recommendations on Baseline Capabilities

National cooperation – Law enforcement

- National/governmental CERTs should establish a clear framework for cooperation with national law enforcement authorities, making sure it is aligned with national regulations on investigations. Where frequent cooperation occurs, the national/governmental CERT should consider formalising the process by defining procedures to ensure that cooperation with law enforcement authorities follows a formal, legal process.
- National law enforcement authorities should have cooperative procedures with European and international law enforcement authorities in place and should be able to facilitate the process of cooperation between a national/governmental CERT and European and international law enforcement authorities.

National cooperation – Policymakers

- In the absence of a national information and cyber-security strategic centre, the national/governmental CERT should provide technical and strategic advice on cyber-security matters to policymakers.

National cooperation – Other CERTs

- A national/governmental CERT should consider striving to maximise its cooperative relationships with domestic CERTs and other incident management or abuse handling teams. To attain this objective, the national/governmental CERT should consider organising a CERT or incident management community or working group.

National cooperation – Military and intelligence

- Cooperation and information sharing between national/governmental CERTs and the military and intelligence communities should be promoted. Such cooperation is mutually beneficial and enhances the overall national capabilities for CIIP and cyber defense. In order to facilitate cooperation with the military and intelligence communities, the staff and communication channels of national/governmental CERTs should have the appropriate security clearances.
- The convergence of cyber-security risks to the military and national governments calls for further work in clarifying the difficult questions that remain, so that a strong coordinated approach on the national and supranational level can be identified.
- The sharing of good practices should be promoted.

Cross-border cooperation

- National/governmental CERTs should consider joining the appropriate structures for cross-border cooperation for national/governmental CERTs, in order to participate actively and contribute to the further development of these structures.

Initiatives in cooperation

Cross-border cooperation – Initiatives in cooperation

- National/governmental CERTs should consider joining appropriate regional, European and international initiatives in cooperation, in order to participate actively and contribute to the further development of these initiatives. Due to the global character of the propagation of internet and security threats, successful cooperation among CERT teams located in different countries in many regions is a key factor for the successful handling of incidents.

Sector working groups

- National/governmental CERTs should consider joining the appropriate sectoral groups for cooperation and should consider participating and contributing actively.

Crucial elements for cooperation – Trust

- On a national level, the national/governmental CERT should build relationships of trust with domestic CERTs and other domestic organisations (e.g., law enforcement agencies, national security or intelligence agencies, the operators of critical information infrastructure, etc). If necessary the national/governmental CERT should consider organising or promoting the organisation of one or several communities for cooperation with a sector specific focus or common objective.

- On an international level, national/governmental CERTs should engage in trust building activities and cross border cooperation, and should consider membership of international or European CERT associations and alignment with relevant CERT accreditation schemes.

Crucial elements for cooperation – Quality of information

- The information that can and should be disseminated to stakeholders should be clearly defined.

- In order to ensure the relevance, completeness and clarity of information in the context of cooperation with relevant stakeholders, national/governmental CERTs should define and adhere to information quality standards such as exchange and naming schemes.

Annex VII: List of original policy recommendations on Baseline Capabilities

- To ensure the security of information, national/governmental CERTs must implement security measures that ensure the confidentiality, integrity, availability and authenticity of information.

Crucial elements for cooperation – Sustainable reaction

- One of the ultimate objectives of a national/governmental CERT is to provide a sustainable and timely reaction to the inputs it receives. In order to reach that level, an adequate level of maturity in policies, processes, technology and people is required.

Crucial elements for cooperation – Common terminology and schemes

- To facilitate national/governmental CERTs cooperation, the adoption and use of common or standardised practices should be promoted for:
  - incident and vulnerability handling procedures;
  - incident, vulnerability and information classification schemes;
  - taxonomies for metrics;
  - information exchange formats (on vulnerabilities, incidents, and system naming conventions);
- To promote international cooperation and prevent isolation or unnecessary or complicated conversions when exchanging information internationally, international standards should be preferred over domestic standards (where appropriate).

Contact details

To contact ENISA for this report please use the following details:

Email: opsec@enisa.europa.eu

Internet: http://www.enisa.europa.eu

enisa
European Network
and Information
Security Agency

PO Box 1309 71001 Heraklion
Greece
Tel: +30 2810 391 280
Fax: +30 2810 391 410
Email: info@enisa.europa.eu

www.enisa.europa.eu

Follow ENISA on

Facebook Twitter LinkedIn YouTube and RSS feeds