enisa
European Network and Information Security Agency

Status Report 2012

Deployment of 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

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.

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, tasked 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

Table of Figures

List of Tables

1

Executive summary

1

Executive Summary

National/governmental computer emergency response teams (n/g CERTs) are teams that serve the government of a country by helping to protect the critical information infrastructure. N/g CERTs play a key role in coordinating incident management with the relevant stakeholders at national level. They also bear responsibility for cooperation with the national/governmental teams in other countries.

This document will familiarise the reader with the current situation in Europe with regard to the n/g CERTs' capabilities, and how these capabilities are deployed.

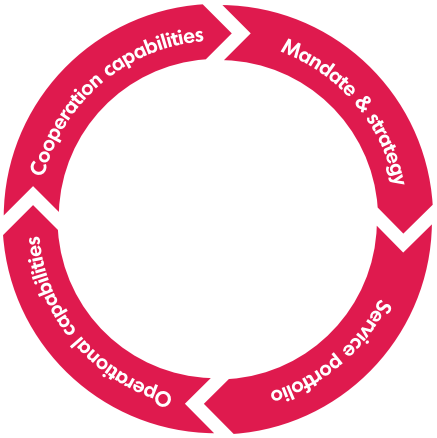
The status of the current situation was assessed according to previously defined categories of capabilities (4) drawn up by ENISA and accepted by the CERT community. Before reading this report it is advisable to consult the previous two documents ENISA published in 2009 and 2010 in order to better understand the complexity of this topic[1].

1 http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities

1. Executive Summary

ENISA's goal is to continuously support the Member States in enhancing and strengthening the cooperation among n/g CERTs in order to achieve a powerful incident response when it is needed. **The key obstacle to cross-border cooperation and incident response that we have identified in recent years is the diversity of capabilities across Member States. Some teams do not have an 'adequate level of maturity' compared with the teams that exist in some other Member States.**

Four baseline capabilities were therefore identified and remain the focus of our research and detailed analysis in this report. The core of the document is structured into four main chapters accordingly: mandate & strategy, service portfolio, operational and cooperation capabilities. At the end of each chapter is a list of identified gaps and possible shortcomings related to each capability. **In the accompanying report, 'Baseline Capabilities of national/governmental CERTs – Updated Recommendations 2012,' the reader will find the recommendations on how to best resolve them.** The shortcomings relate mostly to issues such as questions of clarity, and governmental CERT roles and responsibilities or lack of funding and missing resources (highly specialised IT personnel as well as legal and PR experts).



Key findings concerning the mandate & strategy as the first identified capability:

The role of n/g CERTs is usually supported by a mandate (only two n/g CERT respondents did not refer to any kind of mandate), the details and form of which vary greatly across Member States. A great deal of work needs to be done regarding the proper inclusion of n/g CERTs in national cyber-security strategies: at the time of writing of this report, national cyber-security strategies had been worked out in less than 50% of the Member States.[2] On the other hand, 90% of n/g CERTs are involved, mainly in a consultative role, in the development of laws and strategies on cyber-security. Although there are many variations concerning the hosting organisations of n/g CERTs, several Member States built on the previously observed trend to create national cyber-security centres, which will be ultimately responsible for the implementation of cyber-security strategies integrating the functionality of n/g CERTs.

Key findings concerning the service portfolio as the second identified capability:

The scope of support (proactive services, reactive and security quality management services) the teams provide depends on the type of constituent (or customer). Key constituents such as governmental bodies receive the complete scope of the service portfolio, while a subset of services is available for other constituents, including end-users. Many n/g CERTs have developed valuable expertise in the cyber-security area, which is sought after by law enforcement agencies (LEAs) and other stakeholders in their countries. At least 90% of n/g CERTs organise or take part in seminars on these topics. Some developed and well-established n/g CERTs are able to provide additional services beyond their usual scope of activities for their constituents. This includes, for example, conducting awareness raising projects on behalf of the government or acting in a coordinating role for the national cyber-security exercises.

2 For an overview of national cyber-security strategies in EU Member States see the report from an ENISA project whose aim is to draft a Good Practice Guide on how to develop, implement and maintain a national cyber-security strategy: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper.

Key findings concerning the operational capability as the third identified capability:

More than 80% of n/g CERTs employ 6–8 or more full-time equivalents, which is the minimal staff level considered necessary to provide an acceptable level of service. Even in countries where staff numbers are still officially below this threshold, n/g CERTs usually can count on employees of the hosting organisations in times of need, so that core services are not compromised. However, in smaller teams, the personnel often have to carry out several roles at once, which is a barrier to specialisation. Overall, n/g CERTs report difficulties in hiring high-qualified staff in areas like digital forensics and reverse engineering.

With only a few exceptions, due largely to the fact that the teams concerned were recently established, n/g CERTs provide on-call duty service for incident reports outside of business hours, consisting of various forms of contact points including redirecting calls or email messages on incidents to the staff on-call. PGP-encrypted emails are still the preferred option for communication by n/g CERTs. The teams are located in premises that fulfil the safety requirements associated with the task of processing sensitive information and measures are also taken to ensure that there are back-ups in electronic communication tools in the event that a service provider's connection is down. N/g CERTs' limited budgets often do not allow for significant investments that are needed to provide additional and innovative services such as holding national cyber-security exercises or awareness-raising campaigns. Nevertheless, the necessary staff training and education is taken care of mostly within the teams, including participation in international seminars and conferences.

Key findings concerning the cooperation capability as the fourth identified capability:

It is on the international stage that the n/g CERTs are increasingly visible, which is a necessary prerequisite as the nature of large-scale cyber-incidents and the need to handle them are both national and international in nature. Member States have their n/g CERTs anchored in international structures such as FIRST, TF-CSIRT, EGC, Trusted Introducer, APWG or ENISA workshops and initiatives and the teams serve as the national point of contact for their counterparts. As for cooperation at the national level, both formal and informal approaches are still used. Formal approaches followed include having the n/g CERT meet their constituents (other CERTs, public institutions, critical information infrastructure owners, law enforcement agencies, IT research institutions etc.), in some cases 2–3 times a year, and/or organising working groups. Still, some constituents, especially from the private sector, are sometimes rather unwilling to cooperate and hand over data as they have concerns about the protection of the data. Thus, n/g CERTs are generally in favour of having standardised formats for data information exchange with their peers and would support this idea in international forums. At the same time, though, they do not want to make these standards too rigid but regard them as a baseline set of expectations.

Despite obvious progress in deployment of baseline capabilities across Europe, there are still several challenges which need to be addressed by many interested parties such as legislators, teams themselves, cooperation partners, international initiatives and – last but not least – ordinary citizens.

2

Introduction

2

Introduction

States all over the world rely to a high (and ever increasing) degree on well-functioning critical information infrastructure (CII).[3] However, CII is also significantly affected by breaches of cyber-security as a result of malicious activities. In this regard there is a strong need for efficient n/g CERTs, which are able to effectively handle and respond to attacks on CII and thus contribute to national security in their countries. N/g CERTs[4] play a key role in coordinating incident management with the relevant stakeholders at the national level to secure CII protection. They also bear responsibility for cooperating with the national and governmental teams in other countries that act as official national points of contact. 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 It includes the systems, services, networks and infrastructures that form a vital part of a nation's economy and society, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures. CII includes the public telephone network, the Internet, and terrestrial and satellite wireless networks. They are regarded as critical information infrastructures since their disruption or destruction would have a serious impact on vital societal functions.

4 For definitions of the terms 'national', 'governmental', 'national/governmental' and 'de facto national' CERT see glossary (Annex 1). The term national/governmental CERT was introduced to cover the different types of national, de facto national and governmental CERTs. Note that definitions may vary across Member States.

2. Introduction

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

In its **Communication on Critical Information Infrastructure Protection,**[5] 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'**,[6] 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 (CERTs) should be established in Europe by 2012.*

In its Communication **'The EU Internal Strategy in Action: Five steps towards a more secure Europe'**,[7] the European Commission stresses ENISA's role in improving Member States' capabilities for dealing with cyber-attacks:

> *Member States together with ENISA should [...] undertake regular [...] exercises in incident response... Overall, ENISA will provide support to these (listed before) actions with the aim of raising standards of CERTs in Europe.*

Since 2005, ENISA has run a programme dedicated to supporting n/g CERTs. The goals of this programme are the proliferation of CERTs in Europe in general, to support EU Member States in establishing and developing their n/g CERT capabilities according to an agreed-upon baseline set of capabilities, to foster and to support the cooperation of CERTs on a national and cross-border level and to generally support and reinforce the operation of CERTs and cooperation by making available good practices under the scope of CERTs' activities.

At the national level, Member States are developing their national cyber-security strategies (NCSS), as well as basic tools to improve the security and resilience of CII. It is crucial that these strategies also include provisions regarding the roles of n/g CERTs. In fact, n/g CERTs should be a key component of a NCSS as well as for CIIP strategies.[8]

5 '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

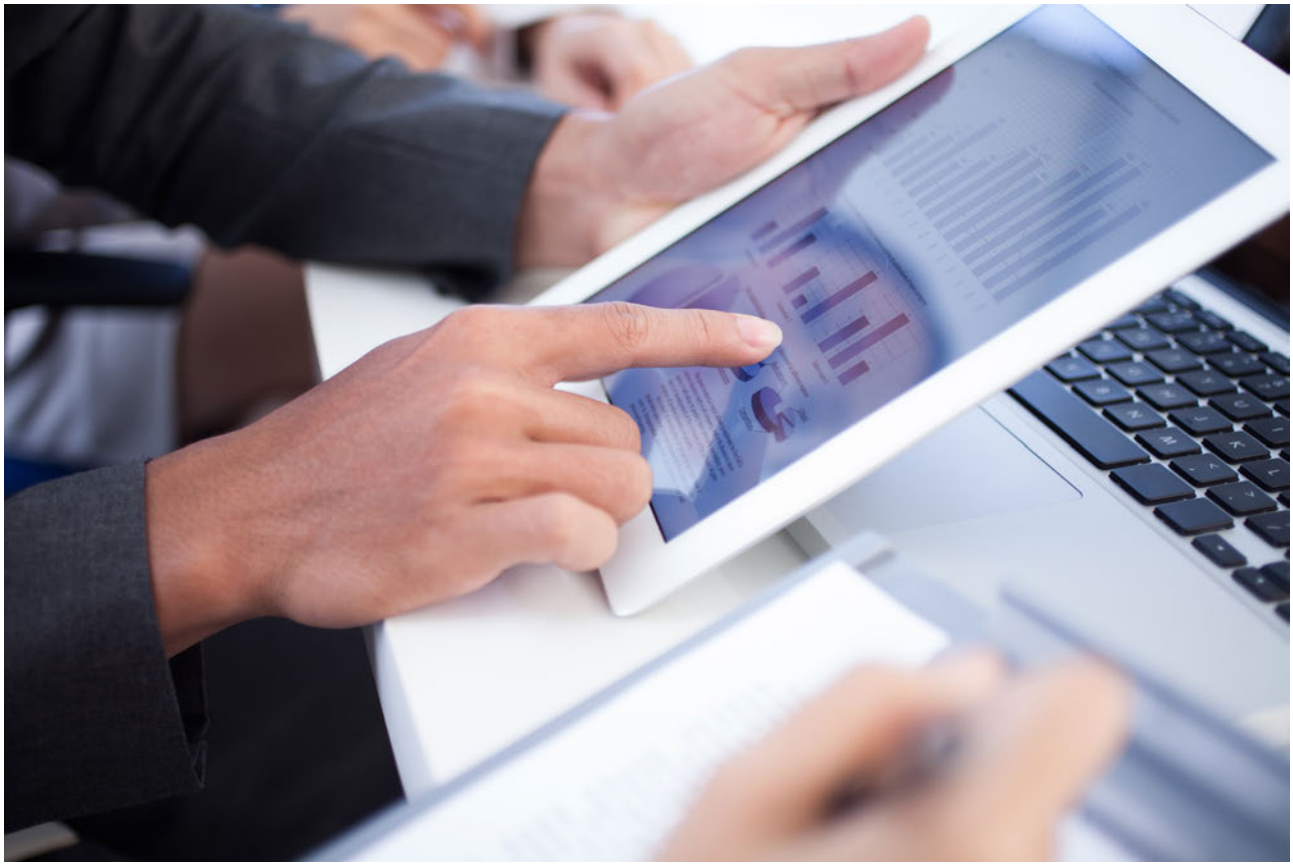
6 'A Digital Agenda for Europe' (COM(2010) 245): http://ec.europa.eu/information_society/digital-agenda/index_en.htm

7 'The EU Internal Strategy in Action: Five steps towards a more secure Europe' (COM(2010) 673): http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf

8 ENISA is monitoring the process of drafting NCSSs with the ultimate aim of preparing a Good Practice Guide on how to develop, implement and maintain an NCSS. The Good Practice Guide is intented to be a useful tool for those responsible for and involved in cyber-security strategies.

2.1 Rationale

In 2009 and 2010 ENISA carried out its first project to define a minimum set of baseline capabilities[9] 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 IT 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 (in areas like mandate, service portfolio, operations or cooperation) can vary substantially across Member States. Diversity in capabilities could negatively influence effective cooperation among n/g CERTs. For the reasons mentioned above, ENISA has launched a project with the aim of reviewing the defined set of baseline capabilities, assessing their adequacy for the current environment as well as the level of deployment in the Member States.



9 http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities

2.1.1 Background information and motivation

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 this report);
- 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 a separate report 'Baseline Capabilities of national/governmental CERTs – Updated Recommendations 2012').

The overall aim 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 all aspects of their work are closed as far as possible.

The original Baseline Capabilities document consists of two parts. Rather concise recommendations on baseline capabilities, created in 2009, are of an operational/technical nature and have been very well accepted by the CERT community. In 2010 ENISA made further improvements and presented a comprehensive set of policy recommendations regarding baseline capabilities of n/g CERTs.

In this report on deployment as well as in the accompanying report on the updated set of baseline capabilities recommendations, 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.

For a detailed list of individual aspects and indicators selected for each capability that are used to measure the current deployment of baseline capabilities, please see section 3.2.1 of this report.

2.1.2 Target audience

The intended target audience for this report (apart from n/g CERTs) primarily consists of ENISA, policymaking bodies at the 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.

2.1.3 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 operations.[10] This report uses several outcomes in the form of recommendations and suggestions from the latest reports. Apart from the original Baseline Capabilities document these included, for example, the following:

- *A flair for sharing – encouraging information exchange between CERTs (December 2011)*[11]

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

- *CERTs Operational Gaps and Overlaps (December 2011)*[12]

This document analyses operational gaps and overlaps of n/g 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)*[13]

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.

10 These activities are futher supported by other intiatives including organising (since 2005) annual workshops for n/g 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.

11 https://www.enisa.europa.eu/activities/cert/support/legal-information-sharing

12 https://www.enisa.europa.eu/activities/cert/other-work/files/operational-gaps-overlaps

13 https://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 n/g 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[14] as well as contributions of experts from an informal expert group. Further details on these sources are provided in the following sub-sections.

3.1 Desk Research

The project team relied mostly on secondary sources to gather information for the project until completed questionnaires were returned from respondents 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 an internal report on deployment. Many CERTs are publishing a good deal of information on their websites in English, including the RFC 2350 documents.[15] Additionally, some information was generated by content from the websites of CERT associations and initiatives such as FIRST and Trusted Introducer[16] 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 section 2.1.3). These ENISA reports were used in conjunction with reports that are still being drafted but which have some preliminary results not published, which have provided 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 an illustrative list of secondary sources used for this report, please see Table 1. Further details are included in Annex III: Web resources.

14 http://www.first.org/

15 These RFC 2350 documents present a basic information tool regarding contact details, scope of services, level of support provided or reporting forms of the CERTs. See Expectations for Computer Security Incident Response: http://www.ietf.org/rfc/rfc2350.txt.

16 http://www.trusted-introducer.nl/teams/updates.html

Table 1:
Main secondary sources

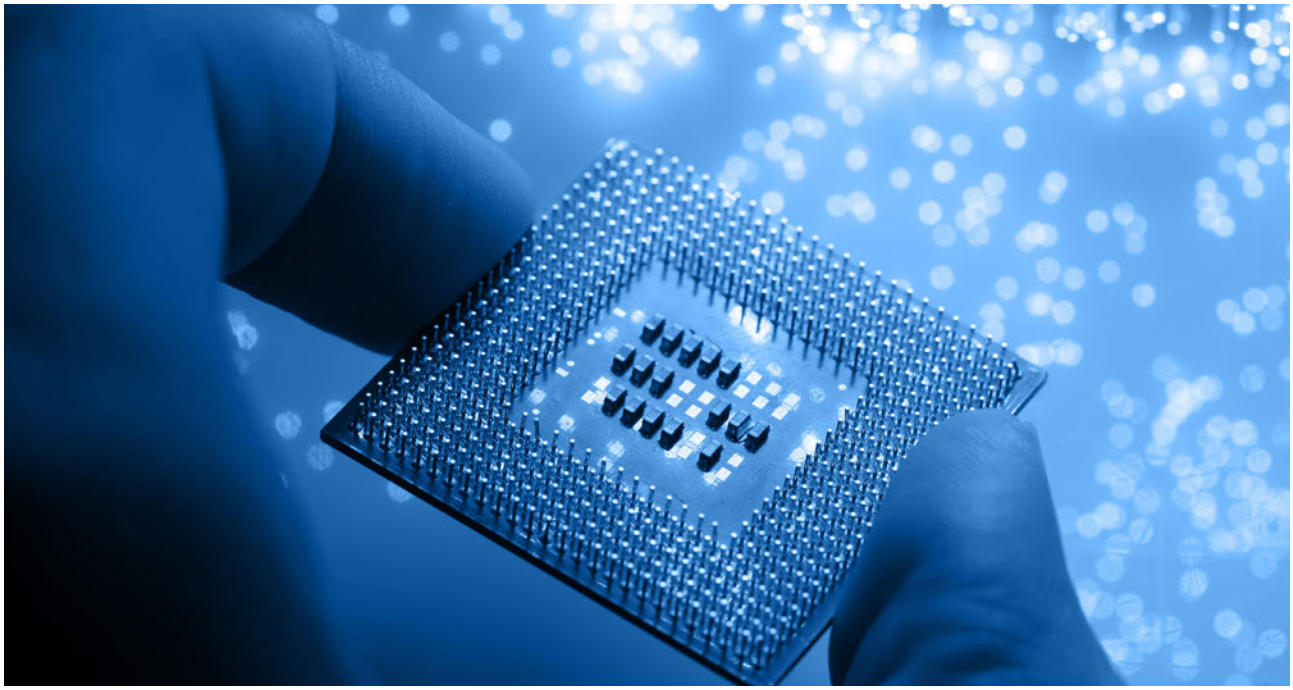
Source
Websites of national/governmental CERTs and other CERTs in the Member States of the EU and EFTA
Websites of policymakers and other stakeholders the area of cyber-security strategy in the EU and EFTA Member States
Document: Baseline Capabilities for national/governmental CERTs (operational aspects and policy recommendations)
Document: Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime – A first collection of practices (ENISA)
Document: A flair for sharing – encouraging information exchange between CERTs (ENISA)
Document: CERT operational gaps and overlaps (ENISA)
Document: CSIRT set-up guide (ENISA)
Document: Good Practice Guide on Incident Reporting Mechanisms (ENISA)
Document: Good Practice Guide for National Exercises (ENISA)
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)

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 main focus of the reports) and the other for other stakeholders (all other CERTs, regulators, policymakers, ISPs and telecommunication operators). The reason for developing such an extensive questionnaire was to collect stakeholders' input for two reports – this report on deployment as well as for the accompanying report on the updated set of baseline capabilities. The full versions of the questionnaires 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 theory (opinions of the n/g CERTs) with practice (opinions of their constituents) and thus delivering the real picture on the activities of n/g CERTs in EU Member States.

3.2 Survey



In total, more than 240 respondents[17] 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 n/g and other CERTs from the ENISA CERT inventory[18] received the introductory letter and the questionnaire. The survey was distributed to other stakeholders such as policymakers, regulators, operators, vendors and others using email lists of ENISA 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, with a focus on n/g CERTs in order to achieve a high response rate. The total final number of returned questionnaires reached 45 (by the beginning of August), of which 25 were from n/g CERTs including the CERT for EU institutions 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 to the type of organisation and country of origin see Figure 1.[19] For an overview of n/g CERTs in all EU and EFTA Member States see Table 2.

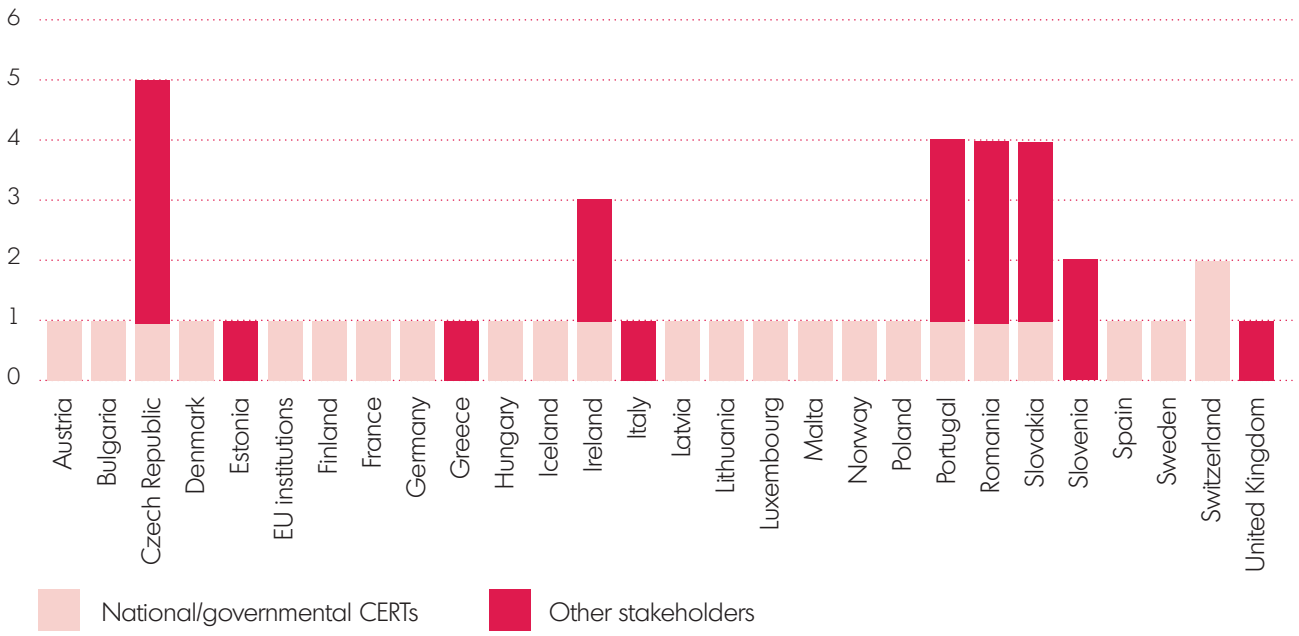
17 This number is cleared from invalid or double contacts, because in some cases the contacted person was no longer working in the organisation contacted, the organisation no longer existed or was merged with or transformed into other organisation, etc.

18 https://www.enisa.europa.eu/activities/cert/background/inv

19 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.

Figure 1:

Survey respondents by country and type of organisation



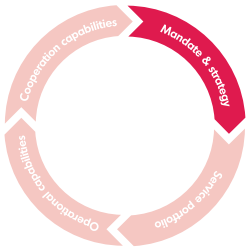
n=45 (25 n/g CERTs plus 20 other stakeholders)

3.2.1 Indicators for the analysis

The questionnaire that ENISA used for the survey of n/g CERTs and other stakeholders was designed in such a way as to collect indicators that would form the basis of the analysis needed to determine the level of deployment of baseline capabilities of n/g CERTs. For each category of capabilities, a group of key indicators was selected, which individually highlight selected aspects of the respective capabilities and their level of deployment. The full analysis of deployment of current baseline capabilities is the subject of chapter 4, Main Findings and Conclusions. The indicators used as a basis for the analysis are listed below along with the objectives of each indicator.

3.2.1 Indicators for the analysis

Mandate & Strategy



Source of mandate – identify whether the mandate of the n/g CERT is based on a national cyber-security strategy, legislative instrument, 'memorandum of understanding' (MoU), government contract or any other source.

Duration of mandate – determine for how many years the mandate for n/g CERT is defined, when it will expire (if applicable), or on what basis it is renewed.

Services outside the mandate – identify whether all services provided by the n/g CERT are covered by the mandate, or whether there are services provided outside the mandate.

Need for mandate clarification – establish whether all roles and responsibilities of the team are clearly defined in the current mandate or whether changes need to be made to clarify the mandate.

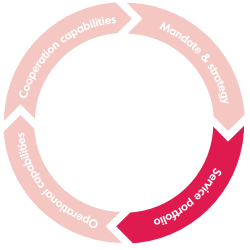
Involvement in national cyber-security strategies and CIIP – understand involvement of n/g CERTs in the national cyber-security law/strategy development and the risk management process for CIIP.

Hosting organisation and its role in the national cyber-security strategy – characterise the hosting organisation of the n/g CERT including their responsibility for a cyber-security agenda and their direct line of accountability to an appropriate section within the government in case of a cyber-security crisis.

Changes to strengthen the mandate – provide information on new measures being developed that will impact the n/g CERTs' mandate. This also serves to gather the views of the teams on how their mandate should be strengthened to support CIIP.

Official point of contact (PoC) for CERTs from other Member States – determine whether the n/g CERTs act as an official PoC for other CERTs (and also for other stakeholders) and whether this role is formally specified in the mandate.

Service Portfolio



Constituencies for national/governmental CERTs – identify the constituencies of the n/g CERTs.

Incident handling and other reactive services – analyse the scope of reactive services provided by n/g CERTs.

Proactive services – analyse the scope of proactive services provided by n/g CERTs.

Services provided beyond basic scope – this indicator helps to identify whether the n/g CERT provides services considered new within the typical CERT services portfolio.

Outsourcing – identify services that n/g CERTs outsource to third parties.

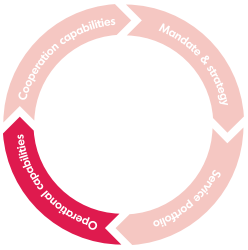
Involvement in Disaster Recovery Planning for CIIP – assess the level of active involvement of n/g CERTs in business continuity management and disaster recovery planning.

Educational and training services – the use of this indicator provides insights into advanced education and training on best practices in cyber-security that the n/g CERTs deliver to their constituents (e.g. national cyber-security exercises involving key constituents such as CII operators).

Sustainability of current scope of services – gather stakeholders' opinions on the relevance of the current services provided by n/g CERTs and the need to add or abandon some services to enhance effectiveness of the teams.

3.2.1 Indicators for the analysis

Operation



Funding model – identify funding models for n/g CERTs and sufficiency of funds regarding the defined scope of work.

Size of staff, its composition and responsibilities – provide information on the current size of staff, its composition including responsibilities allocated to individual staff members as well as identification of staff needed and missing in the n/g CERTs.

Training of staff – describe the options for staff training (internal, national, European, international) of the n/g CERT.

Communication means and their security – gather details on means of communication available to constituents and third parties to contact the n/g CERTs as well as on the level of security implemented.

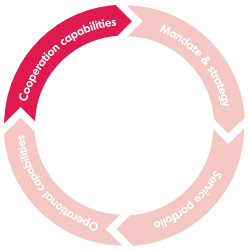
24/7 availability in place – provide details on n/g CERTs' availability on 24/7 basis (on-call duty, shifts).

Physical security measures – identify measures to safeguard premises of the n/g CERTs.

Information quality standards and service management improvement processes – gather information on quality standards applied by n/g CERTs such as exchange and naming schemes. At the same time, it also addresses service management and quality systems/processes designed to follow up on and improve performance.

Best practices and CERTs' role in dissemination of terminology – identify the main sources for best practices employed by the n/g CERTs as regards incident reporting forms or incident handling procedures. It is also used to determine the n/g CERT's role in defining and disseminating terminology within the national cyber-security community.

Cooperation



Membership in CERT structures and initiatives – outline the engagement of n/g CERTs in international CERT structures and initiatives and the benefits that they gain from these memberships.

Bilateral cooperation – assess the teams' engagement in formal and informal bilateral partnerships with their peers in EU Member States.

Trust criteria for cooperation with national/governmental CERTs – characterise trust criteria applied by n/g CERTs for their peers in other countries.

Enforcement powers – establish whether the n/g CERT can require its constituents to implement measures to counter cyber-security threats.

Cooperation with LEAs – characterise the framework for cooperation between n/g CERTs and law enforcement agencies.

Working groups and associations for domestic stakeholders – describe the procedures for cooperation between n/g CERTs and other domestic CERTs and stakeholders.

Special requirements for CII bodies – focus on the views of n/g CERTs regarding different requirements for specific constituents such as CII operators.

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 for the general interview guide), but 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 telephonically (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 on average about one hour. 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[20] of the FIRST association took place in Malta.[21] A project team member, who also took part in the conference, established valuable contacts with a number of n/g CERTs with the support of ENISA. The contractor engaged in talks (not full-scale interviews due to limited time available during conference sessions) with several national/governmental CERTs at the conference and 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 of 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 experts representing the n/g CERTs, other CERTs, and other stakeholders who volunteered to take part in an 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.

20 http://www.first.org/events/first

21 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.

4

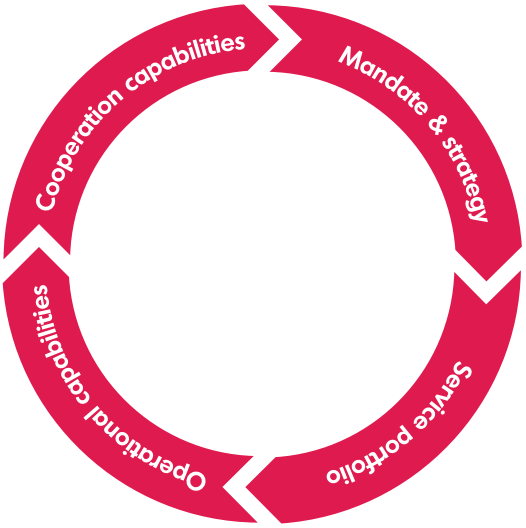
Main Findings and Conclusions

4 Main Findings and Conclusions

4.1 Background for the Analysis

In this chapter, an overview is provided on the current status of deployment of baseline capabilities for n/g CERTs in EU Member States. The capabilities are organised into four key categories:

- **Mandate & strategy** relates to the powers and justification in the 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 that a team must comply with; and
- **Cooperation capabilities** encompass requirements regarding information sharing with other teams that may be partly covered by the previous three categories.



For each of these categories, the report provides an overview that is further elaborated upon according to individual topics and themes, largely following the main content of questions of the survey conducted among n/g CERTs (for details on indicators/topics selected see section 3.2.1). At the end of each subchapter there is a conclusion assessing the overall level of deployment of the respective capability and identifying outstanding gaps. These gaps are further handled (with recommendations on how to close them) in the accompanying report 'Baseline Capabilities of national/governmental CERTs – Updated Recommendations 2012'.

The findings relate to n/g CERTs in 27 EU Member States plus 3 EFTA countries (Iceland, Norway and Switzerland). The n/g CERTs in these countries plus a CERT for EU institutions are listed in alphabetical order in Table 2: Overview of national/governmental CERTs in Europe (EU and EFTA Member States).[22] The vast majority of Member States have already established n/g CERTs, although there are significant differences regarding the power of their mandate, their role in developing national cyber-security strategies, the type of CERT (i.e., national, de facto, national/governmental, governmental), years of operation and the resulting maturity status of the team.[23]

22 For a list of CERTs across Europe please consult ENISA's Inventory of CERT activities in Europe and CERTs in Europe map.

23 Except Italy and Cyprus, where at the time of writing there is no official n/g CERT in operational mode. The situation is unclear in a few other countries as well, although they have an n/g CERT on paper. In a few countries there are also more CERTs which act at national (national TLD) or governmental level.

4.1 Background for the Analysis

Table 2:

Overview of national/governmental CERTs in Europe (EU and EFTA Member States)*

Country	Name of n/g CERT	Website
Austria	CERT.AT (including the GovCERT.gv.at function)	http://www.cert.at/ and http://www.govcert.gv.at/
Belgium	CERT.BE	https://www.cert.be/
Bulgaria	GOVCERT.BG	https://govcert.bg/
Cyprus	Ongoing project to set up the n/g CERT	http://www.ocecpr.org.cy/
Czech Republic	CSIRT.CZ; and ongoing project to set up the governmental CERT	http://www.csirt.cz/
Denmark	GOVCERT.DK	https://www.govcert.dk/
Estonia	CERT-EE	http://www.cert.ee/
European Union institutions	CERT-EU	http://cert.europa.eu/cert/
Finland	CERT-FI	http://www.cert.fi/en/
France	CERTA	http://www.certa.ssi.gouv.fr/
Germany	CERT-BUND	https://www.cert-bund.de/
Greece	NCERT-GR	http://www.nis.gr/
Hungary	CERT-HUNGARY	http://www.cert-hungary.hu/
Ireland	CSIRT-IE	http://www.dcenr.gov.ie/
Iceland	CERT.IS	n/a
Italy	Ongoing project to set up the n/g CERT[24]	n/a
Latvia	CERT-LV	http://cert.lv/
Lithuania	CERT.LT	https://www.cert.lt/
Luxembourg	CIRCL.LU; GOVCERT.LU	http://circl.lu/ and http://www.govcert.lu
Malta	MTCERT; and ongoing project to set up the national CERT	n/a
Netherlands	GOVCERT.NL (NCSC.NL)	https://www.ncsc.nl/
Norway	NORCERT	https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/
Poland	CERT POLSKA; GOVCERT.PL	http://www.cert.pl/ and http://cert.gov.pl/
Portugal	CERT.PT	http://cert.pt/
Romania	CERT-RO	http://www.cert-ro.eu/
Slovakia	CSIRT.SK	http://www.csirt.gov.sk/
Slovenia	CERT.SI	http://www.cert.si/
Spain	INTECO CERT, CCN CERT	http://cert.inteco.es/ , https://www.ccn-cert.cni.es/
Sweden	CERT.SE	http://www.cert.se/
Switzerland	SWITCH CERT and GOVCERT.CH (Melani)	http://www.switch.ch/ and security/ and http://www.melani.admin.ch/
United Kingdom	CSIRT-UK and GOVCERT.UK	http://www.cpni.gov.uk/ and http://www.cesg.gov.uk/policyguidance/GovCertUK/

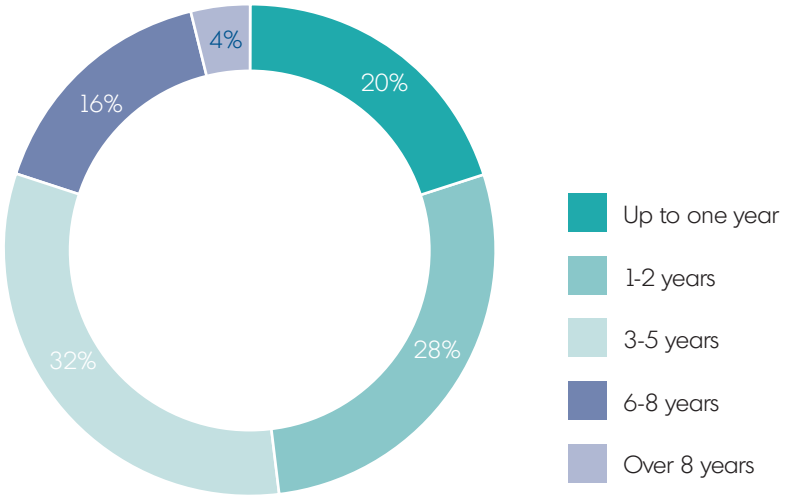
* Please note that Table 2 includes any type of CERT with national or governmental or national/governmental role based on definitions outlined in the survey and included in Annex 1. The list is not exhaustive and is subject to development.

24 ENISA is currently supporting Italy in its efforts to establish a national/governmental CERT based on its request.

4.1 Background for the Analysis

Overall, there is still some confusion over how n/g CERTs perceive themselves and are perceived according to definitions of national, governmental, *de facto* national or national/governmental (see Annex 1: Glossary). The project team identified several instances where the n/g CERTs indicated a different type for their organisation than provided in the ENISA Inventory of CERT Activities in Europe, Version 2.7, 05/2012[25] or the database of Trusted Introducer.[26] Still, a statement can be made regarding the overall balance of national, governmental and n/g CERTs, with a lower number of CERTs being portrayed as *de facto* national.

Figure 2:
Years of operation of national/governmental CERT



n=24 n/g CERTs

Significant differences also exist with regard to the time that n/g CERTs have been operating (see Figure 2). The largest share (32%) of n/g CERTs have been operating between 3 and 5 years, while well established n/g CERTs operating for more than 8 years amount to one-fourth of n/g CERTs in Member States. N/g CERTs established between 6 and 8 years ago and quite new n/g CERTs younger than 2 years are equally represented, both accounting for about one-fifth of CERTs. The longest serving n/g CERTs in the list appear to be those established originally for the purpose of overseeing the national research and educational networks.

The level of deployment of baseline capabilities of n/g CERTs also determines the maturity status of the n/g CERTs.[27] The diversity of the level of development of n/g CERTs across Europe is obvious as each category of the maturity model (initial, repeatable, defined, managed, optimised) is represented among the teams.

The largest portion of n/g CERTs identify their maturity status as being in the middle (defined) range (see Figure 3). This includes the following parameters: being recognised as a national contact point in the international CERT community, having defined and documented standard processes established for main

25 http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

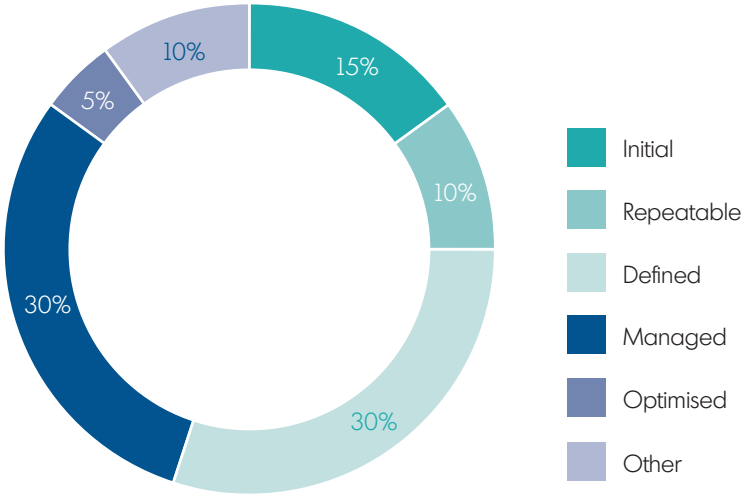
26 https://www.trusted-introducer.org/teams/country_LICSA.html

27 The maturity model of CERTs is based on the Software Capability Model levels defined by the Carnegie Mellon University Software Engineering Institute. See the glossary in the questionnaire for national/governmental CERTs (Annex VII).

4.1 Background for the Analysis

CERT services and providing additional added value CERT services. Almost an equally large group of the teams consider themselves to have already reached the more advanced status on the maturity model (managed) – which is supported by, inter alia, process metrics and having an official mandate for certain n/g CERT responsibilities.

Figure 3:
Self-assessment of the maturity status of national/governmental CERTs



n=20 n/g CERTs

The n/g CERTs that have been set up only recently are in the 'initial' or 'repeatable' phase, respectively. One of the more mature n/g CERTs is of the opinion that it has already reached the highest maturity status – 'optimised'. An n/g CERT having achieved the optimised level should have a full official mandate for all n/g CERT responsibilities and have long-standing excellent trust relationships with its constituency, stakeholders and other n/g CERTs as well as provide mature services and focus on continually improving its process performance.

It is evident that such a self-assessment of maturity status is subjective and there can be a tendency to overrate or, on the other hand, underrate one's own performance. In each case, the teams stated that they are determined to reach the next phase in the maturity model by the end of the year or in a year at the latest. As evidenced by the interviews conducted with n/g CERTs, such a shift will coincide with a new mandate or accomplishment of the membership process at the FIRST association or the accreditation process with Trusted Introducer.

4.2 Mandate & Strategy

4.2.1 Overview

N/g CERTs have been established in the vast majority of EU Member States.[28] Member States mandate their n/g CERTs in several ways: they have national cyber-security strategies[29] in place which mention and specify the role of n/g CERTs (e.g. Slovakia), or they adopt special laws (e.g. Denmark, Greece, Finland, Latvia, Spain and others), which include parts related to n/g CERTs. These laws address several areas: telecommunications regulatory frameworks, personal data protection, and critical infrastructure protection and security. The involvement of n/g CERTs in the development of the above-mentioned laws and strategies is satisfactory (with nearly 90% of n/g CERTs stating to be involved), although the level of involvement varies considerably by country.

Notwithstanding the existence of a national cyber-security strategy or a law, the mandate for n/g CERTs is often part of governmental decrees (e.g. in Hungary, Romania, Slovakia) or regulatory orders (e.g. in Lithuania). The Czech Republic is a special case in that the mandate takes the form of a memorandum between the government and the national domain administrator. There are also countries where no formal mandate appears to have been issued, but the n/g CERT is still carrying out its tasks (e.g. Portugal).

There is still room for improvement regarding the clarity of mandate, as only little more than 60% of n/g CERTs claimed that their mandate covered the basic scope of their services. Lack of clarity of mandate covers, for example, cases where the envisaged scope of services does not correspond to n/g CERTs' capacities. In addition, more details are sometimes needed for n/g CERTs on cooperation with LEAs and the scope and funding of a governmental CERT-part function may also require clarification.

Member States display various patterns regarding the hosting organisations of n/g CERTs. In Finland the n/g CERT is embedded within a national regulatory authority (NRA), which makes it possible for the n/g CERT to take advantage of, for example, an NRA's authority over telecommunications providers in crisis situations. An alternative arrangement for some n/g CERTs (e.g. Malta, Estonia) is to be hosted by IT and information systems authorities. One trend that seems to be global rather than purely European is reflected in the creation of national cyber-security centres responsible for implementation of national cyber-security strategies. These structures have already been implemented in the United Kingdom and the Netherlands, while the newly established Irish n/g CERT is also heading in this direction. Several Member State governments have adopted a holistic security approach and base their n/g CERTs within justice, security and intelligence institutions, either ministries or executive agencies (e.g. France, Greece, Netherlands, Poland, Spain, Sweden).

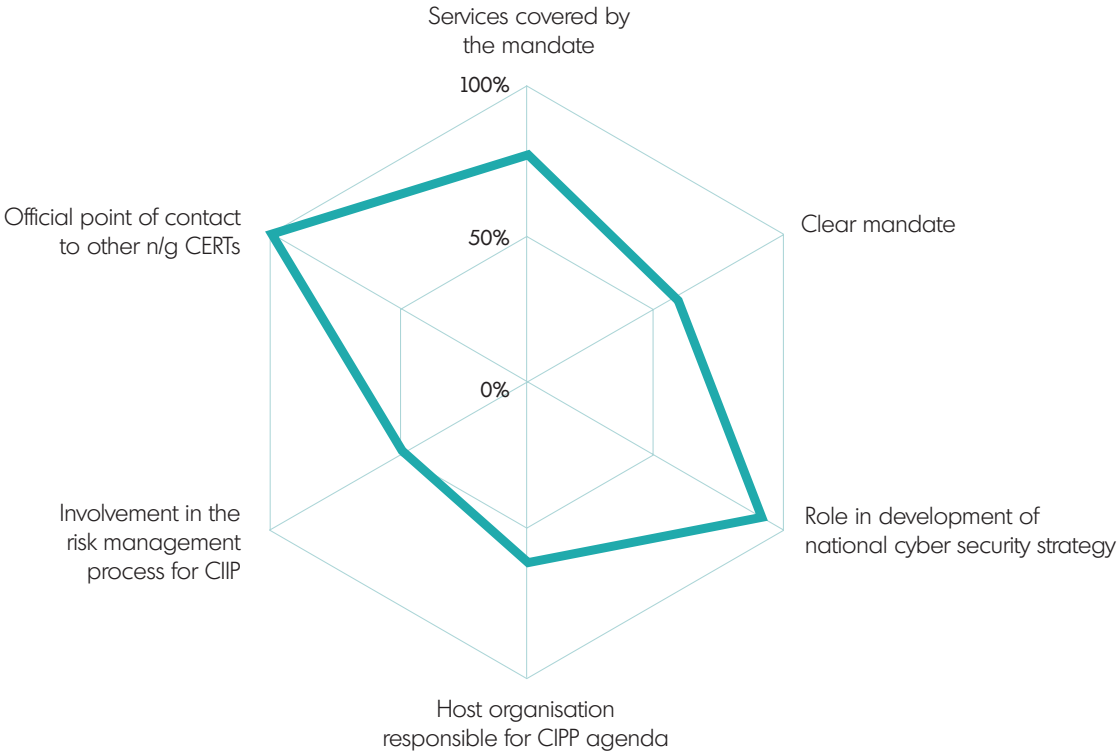
28 It should be noted that in many cases national CERTs also exercise the role of governmental CERTs until the new national cyber-security strategy or law is developed or another new arrangement is finalised.

29 For an overview of national cyber-security strategies in EU Member States see the report from an ENISA project whose aim is to draft a Good Practice Guide on how to develop, implement and maintain a national cyber-security strategy: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper

4.2.1.1 Source of mandate

Figure 4:

Visual scheme of deployment of mandate capabilities



n=25 n/g CERTs

Figure 4 provides an overview on deployment of some aspects of the mandate capability by Member States. As can be seen, the n/g CERTs universally act as *de facto* official points of contacts to their peers in Europe. Also they are to a high degree (appr. 90%) involved in developing national cyber-security strategies. On the other hand, according to 63% of n/g CERTs (and 69% of other stakeholders), the mandate is not clear enough. Gaps also remain in the involvement of the n/g CERTs in risk management process for CIIP (only 50% n/g CERTs claim some involvement) or regarding the objective that the hosting organisations are responsible for CIIP agenda (62% of cases reported).

4.2.1.1 Source of mandate

It is absolutely crucial that the n/g CERTs be given a clear mandate from their governments so that they can officially act as key players for preparedness, information sharing, coordination and response to various kinds of attacks on critical information infrastructure. Member States can provide a mandate to their n/g CERTs in several ways. Where there is a national cyber-security strategy in place (this is the case in only about half of the Member States), the role of the n/g CERT should be outlined.

The more precise scope of a mandate for n/g CERTs is most often included in specific government decisions, decrees and orders (about two-thirds of n/g CERTs). A few n/g CERTs also indicated that their mandate is part of a contract (in one case in the form of a less formal memorandum) with the government. Two n/g CERTs reported that their roles are covered under the responsibilities of their hosting organisations.

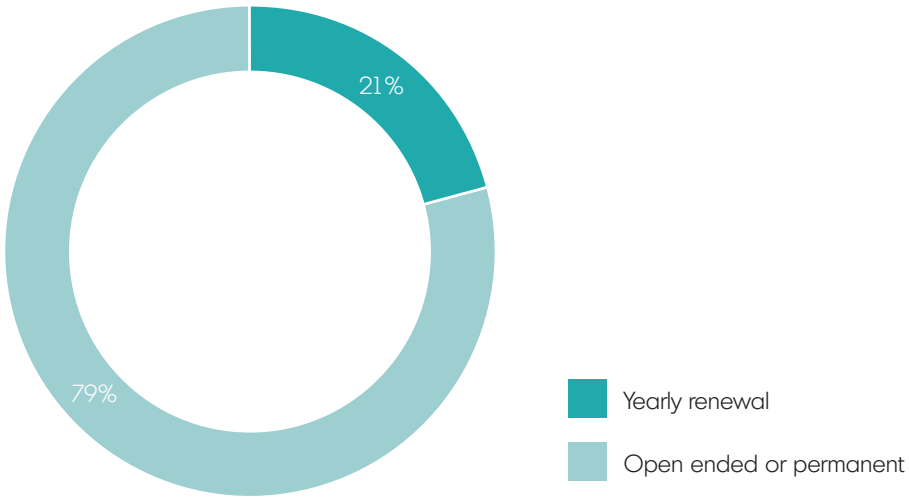
Where there is no link to a national cyber-security strategy (NCSS) regarding n/g CERTs, the mandate or the basic scope of responsibilities of an n/g CERT may be defined in special laws and further specified in the above-mentioned government decisions. These laws refer to several areas: general telecommunication regulatory framework, personal data protection, CIIP or general national security. There are also cases (at least two n/g CERTs) where there is no formal mandate issued but the n/g CERT is still carrying out its tasks.

An interesting observation from other stakeholders (and constituents of n/g CERTs) is that they are sometimes (in two cases) not aware of all the details of an n/g CERT's mandate as the details are not made public. As the mandate usually does not mention any formal structures for cooperation with constituents, they interact with n/g CERTs on an informal basis (more than two-thirds of other stakeholders).

4.2.1.2 Duration of mandate

The mandate for n/g CERTs is not time-limited in a significant majority (nearly 80%) of Member States (see Figure 5). The project team recorded five exceptions: four of them are for Central and Eastern European countries, where it is expected that the mandate will become indefinite once temporary arrangements end, and the other pertains to the CERT-EU for European Union institutions. In all of these cases the mandate is (was) renewed annually. Therefore, a clear trend towards an open-ended mandate can be observed.

Figure 5:
Time scope of the mandate



n=24 n/g CERTs

4.2.1.3 Services outside the mandate

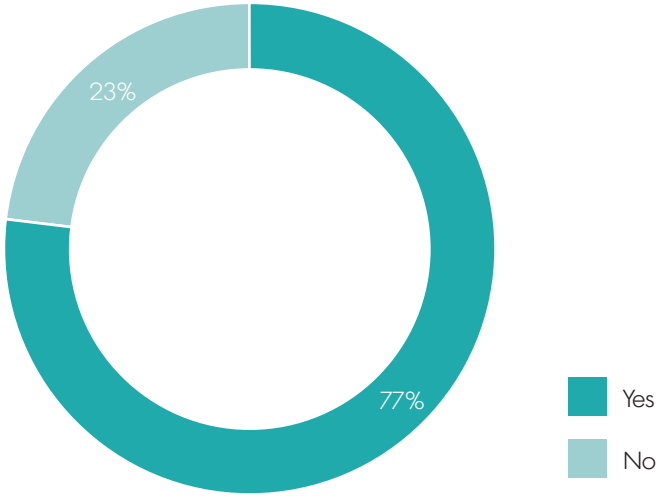
Seventy-seven percent of n/g CERTs are of the opinion that the services they offer are covered by their mandate (see Figure 6). Those n/g CERTs, which identified additional services that they provide outside the scope of their mandate, cited the following services among others:

- training of members of security forces in area of computer security;
- collecting data on detected security incidents originating from the networks operating in the country and sending a request for verification to end networks;
- being a certification authority for Citizens Initiative platform;
- investigation of violations of and threats to information security.

It is evident that the way the n/g CERTs perceive their mandate is rather subjective because essential services provided by n/g CERTs such as serving as their country's official PoC for other n/g CERTs or collecting incident data should usually be covered by the mandate, regardless of the mandate's breadth.

Figure 6:

All provided services considered to be covered by the mandate

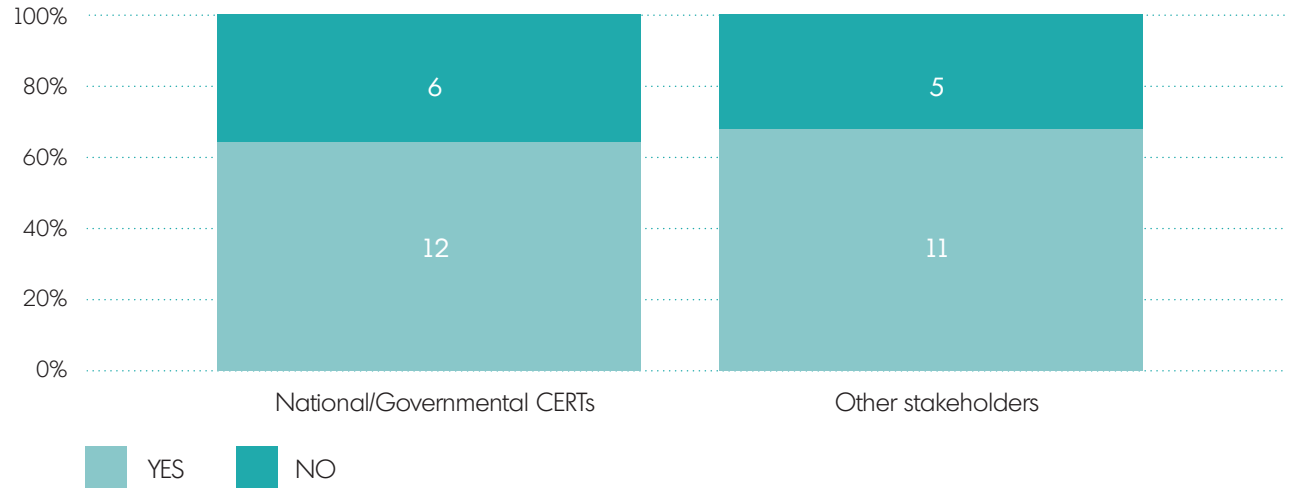


n=22 n/g CERTs

4.2.1.4 Need for mandate clarification

Sixty-three percent of n/g CERTs claimed that the roles and responsibilities of their teams are clearly defined and that no major changes are needed. This is broadly in line with the sentiment of other stakeholders, almost 70% of which agree with this statement (see Figure 7).

Figure 7:
All responsibilities of n/g CERTs considered clear in the mandate



n=34 (18 n/g CERTs + 16 other stakeholders)

The CERTs listed the following areas where problems regarding clarity occur or could occur:

- The scope of services described in the mandate does not correspond to the team's capacity. The project team assumes that this issue will pertain to n/g CERTs with limited staffs, mainly in Central and Eastern Europe.
- Changes with regard to reporting cyber-security incidents may be applied. Although constituents are requested to report incidents, problems can arise when the law is not sufficiently clear and ISPs and operators do not know to whom they should report incidents. Again, this may be the problem that n/g CERTs across Member States experience, this time without any regional distinction.
- Clarification might be required in the future with regard to collaboration with LEAs.
- The provision and funding of the governmental CERT-part capabilities have so far not been adequately addressed. This is a valid point, especially when a national CERT takes on the role of a governmental CERT as well.
- There is a need for n/g CERTs to reach out to more citizens with their services and therefore work on their external presentation/communication.

Despite some sentiment from n/g CERTs that more clarity will come with new strategies and/or laws, the project team also recorded the opinion that mandate should remain general. The reason for this is that it is difficult to predict what additional tasks may come up. Regarding other stakeholders (who are also constituents of n/g CERTs), there is an increased call for formality and empowerment to gain formal recognition and to allocate required resources for supporting a determined cyber-security strategy.

"Each CSIRT/CERT operates in a different environment; each has a different mandate, structure and competences within national borders, which is a great source of discrepancies."

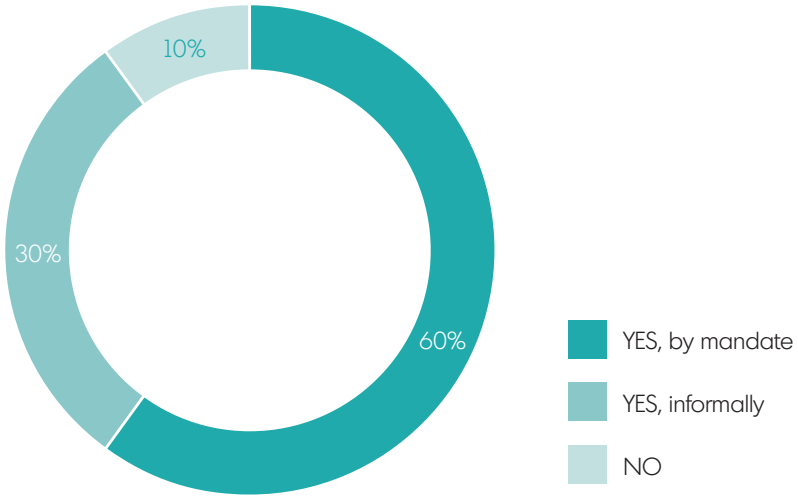
n/g CERT respondent

4.2.1.5 Involvement in national cyber-security strategies and CIIP

According to n/g CERTs, about 60% of n/g CERTs' mandate include a role in the development of the national cyber-security strategy or laws (see Figure 8). This can include the assessment of risks, creation of a risk management plan for CIIP, implementation of the plan, verification of its effectiveness, and regular evaluation and improvement. In a further 30% of cases, n/g CERTs exercise this role informally. This corresponds roughly to the actual involvement of n/g CERTs in developing and drafting national cyber-security laws and strategies. In total, approximately nine out of ten n/g CERTs claimed to be (or have been) involved in developing cyber-security strategies.

Figure 8:

Involvement of n/g CERTs in the development of national cyber-security strategy



n=20 n/g CERTs

However, the level of involvement varies greatly among n/g CERTs in EU Member States. While one n/g CERT stated unequivocally that it is the driving force behind the development of its country's cyber-security strategy and other n/g CERTs claimed very active participation and detailed expertise, in some cases the role is that of formal consultation. Approximately 50% of n/g CERTs claimed that a new strategy/law was being developed that would affect their mandate.

N/g CERTs' level of involvement for the risk assessment process of CIIP drops to just 50% of n/g CERTs. This involvement is usually indirect, with n/g CERTs providing technical expertise and especially real figures about the security of national critical information infrastructures. For example, in one big Member State, the n/g CERT is the central contact point for CII operators and the hosting organisation also has a dedicated section for CII.

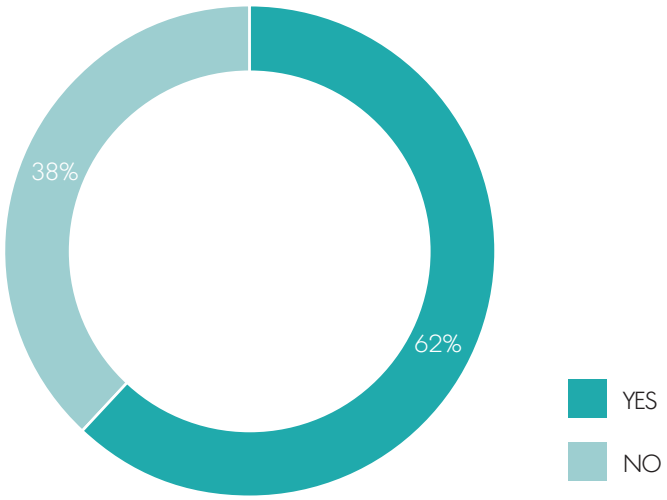
4.2.1.6 Hosting organisations and their role in the national cyber-security strategy

N/g CERTs are typically (90% of respondents) hosted by a higher organisation (ministry, regulatory authority, other government agency, research institute, etc.) It is often useful for an n/g CERT to be embedded within a national regulatory authority (NRA) like in Finland. This arrangement makes it possible to take advantage of an NRA's authority over telecommunications providers in crisis situations, as survey respondents indicated several times.

An intermediate arrangement that Member States can consider is hosting n/g CERTs with IT and information systems authorities. As mentioned before, a trend that seems to be global rather than European is the creation of national cyber-security centres responsible for national cyber-security strategies. For example, these structures have already been implemented in the United Kingdom and the Netherlands, while the newly established Irish n/g CERT is being integrated into this structure and similar developments are under way in the Czech Republic. Several governments have adopted a holistic security approach and base their n/g CERTs within justice, security and intelligence institutions, either ministries or executive agencies (e.g. France, Greece, the Netherlands, Spain, Sweden). Further, there are still hosting organisations of n/g CERTs (e.g. Latvia, Poland or Portugal) that reflect the n/g CERTs' original areas of activities, for example as supervisors of national research and educational networks. More than 60% of hosting organisations of n/g CERTs are responsible for the national cyber-security agenda of their country, including handling of crisis situations and CII protection (see Figure 9). Through the hosting organisations, in the case of a cyber-security crisis (e.g. large scale cyber-attack), the n/g CERTs have a direct line of accountability to an appropriate section within the national executive. In total, more than 80% of n/g CERTs reported either having a formal or informal line of accountability in such cases.

Figure 9:

Hosting organisation of n/g CERTs responsible for cyber-security agenda



n=24 n/g CERTs

4.2.1.7 Changes to strengthen the mandate

Although more than three-quarters of n/g CERTs think that their roles and responsibilities are more or less covered by their mandate (see section 4.2.1.3), a majority of n/g CERTs mentioned ideas to strengthen their mandate in the survey. They mostly referred to new laws and strategies being drafted, which should address issues surrounding mandate. Among the main topics that n/g CERTs mentioned in this respect were the following:

- Requiring operators and ISPs to report incidents;
- Closer involvement in the implementation of Article 13 of the Framework Directive 2009/140/EC;[30]
- Clarifying relations between n/g CERTs and constituents;
- Long-term planning and budgetary issues including a broader funding base;
- Improving and interlinking national regulations on CIIP and electronic communications;
- Stimulating and developing a national CERT community and PPP;
- Allowing n/g CERTs to proactively scan infrastructures and report vulnerabilities to the network owners;
- Regulations allowing the n/g CERTs to handle personal data so that the incident handling process is streamlined;
- Incorporating n/g CERTs into national cyber-security centres while giving the n/g CERTs a central role in facilitating communication with other national agencies responsible for CIIP.

30 Article 13a of the Framework Directive introduces significant new measures to increase the security and resilience of electronic communications networks. These measures are designed to enhance levels of network availability, as well as to protect against and prepare for disruptions to availability. Security requirements are also imposed on electronic communication service providers. These measures only apply to publicly available electronic communications services and not to private networks.

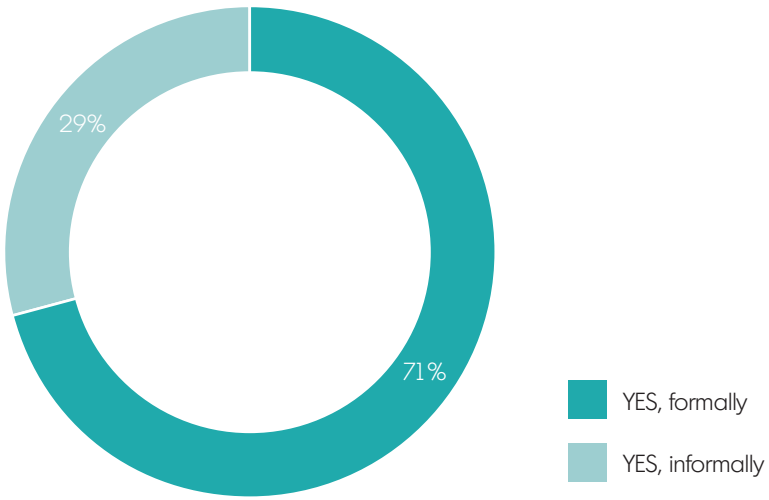
These ideas for strengthening the mandate for n/g CERTs are largely echoed by other stakeholders, although to a lesser degree, with four respondents from this group stating that n/g CERTs do not need any additional powers. Operators were in favour of lessening the bureaucratic burden associated with reporting to both n/g CERTs and NRAs. Constituents stressed the need for n/g CERTs to have more resources to be able to respond effectively to incidents and provide the broad scope of proactive, reactive and security quality management services necessary. There was also a call among other stakeholders for n/g CERTs to be stronger in terms of judicial and police cooperation.

4.2.1.8 Official point of contact for n/g CERTs from other Member States

Acting as the official national point of contact for other Member States' n/g CERTs and worldwide is a specific role of n/g CERTs. An official mandate from its government to represent the country in international CERT communities, such as FIRST (Forum of Incident Response and Security Teams) and potentially EGC (European Government CERTs), is crucial for an n/g CERT.

More than 70% of n/g CERTs (see Figure 10) have the formal status as national PoC, while the rest perform the same role without any formal mandate by acting as 'de facto' PoCs. A vast majority of n/g CERTs also act as national PoC for incident reporting and incident information dissemination. However, unlike at the international level where an n/g CERT can develop a reputation based on taking a proactive approach, the need for an n/g CERT to have an official mandate seems to be stronger on the domestic front.

Figure 10:
National/governmental CERTs acting as official Point of Contact



n=24 n/g CERTs

4.2.1.8 Official point of contact for n/g CERTs from other Member States

Conclusions

The n/g CERTs have been granted a mandate from their governments to carry out tasks of coordinating and supporting incident handling within the state borders and acting as CERTs-of-last-resort domestically and official point of contact for n/g CERTs in other countries. The power and sources of the mandate vary significantly. There is a clear trend of giving the n/g CERTs an indefinite mandate, while the practice of its periodic renewal is being abandoned. Only half of the Member States had accomplished the national cyber-security strategy, but on the other hand 90% of n/g CERTs are or will be involved in the development of these strategies. The teams are hosted in a variety of hosting organisations including policymakers, regulators, research institutes or TLD administrators. In more than 60% of cases these organisations are responsible for the cyber-security agenda.

Regarding the mandate & strategy capability, a number of deployment shortcomings/gaps have been identified, which are further addressed in the accompanying report 'Baseline Capabilities of national/governmental CERTs – Updated Recommendations 2012'. The key identified gaps in the deployment of this capability include:

- The mandate is not always clear enough, so that it cannot support some activities of the n/g CERTs.
- The mandate is often not made public or sufficiently promoted, which creates doubts on roles and responsibilities of n/g CERTs.
- 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.
- Special provisions including funding needs are missing for the governmental CERT-part functionality.
- N/g CERTs face problems of limited authority when requiring ISPs to handle incidents.
- Data protection legislation is another obstacle for effective incident handling management.

4.3 Service Portfolio

4.3.1 Overview

N/g CERTs provide all categories of services stipulated in the original Baseline Capabilities document, which includes proactive services, reactive services and security quality management services. It is obvious that more mature n/g CERTs and those with the most resources are able to provide more extensive services in all of the mentioned categories for key constituents like governmental bodies and CII public operators. Incident management is the only service that is universally provided to the constituents of an n/g CERT. Sometimes there is a perception that certain services are being duplicated with regard to proactive services (like technology watch reports) which are disseminated by other types of CERTs and commercial vendors. This may give the impression of valuable resources being wasted.

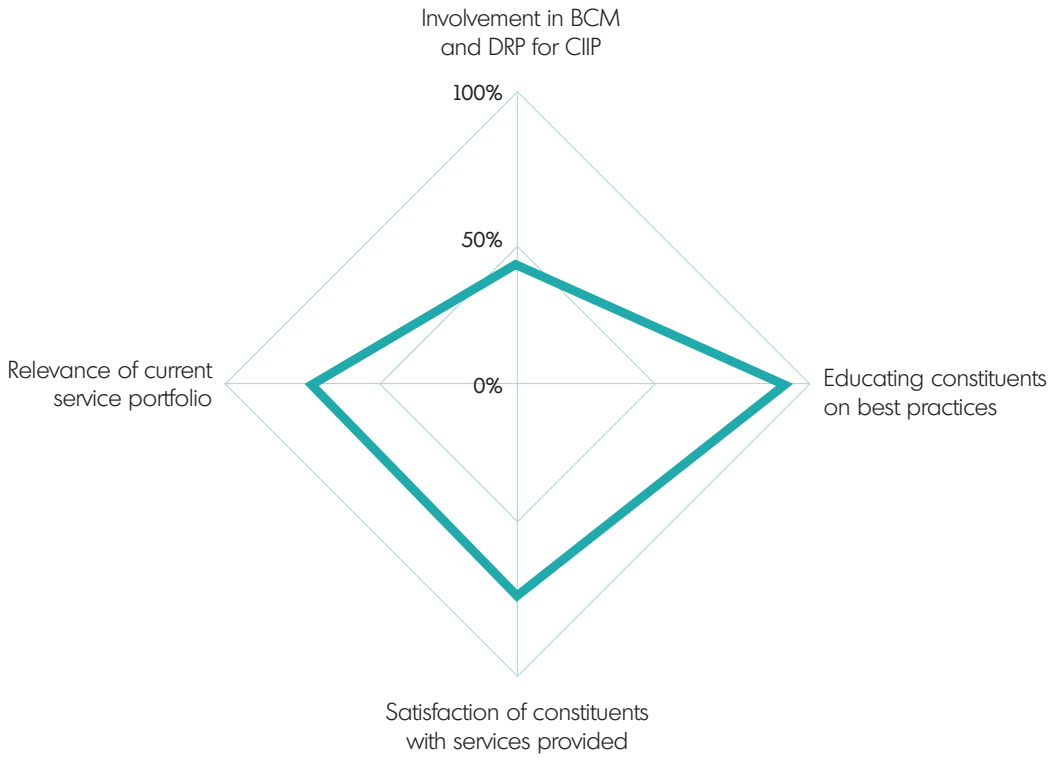
N/g CERTs have gradually developed expertise in cyber-security, which is sought after by stakeholders in this area such as LEAs. Team members are also asked to consult with regard to drafting strategies and laws affecting CIIP. It has also become common for n/g CERTs to organise seminars and workshops and provide tutorials, and around 90% of n/g CERTs are engaged in these activities. On the other hand, only about 40% of n/g CERTs reported that they are involved in disaster recovery planning (DRP) and business continuity management (BCM). The level of involvement varies based on the n/g CERT's mandate and relations with hosting organisations.

Some developed and well-established n/g CERTs are able to provide additional services for their constituents beyond their usual scope of activities. These might include running an awareness raising project or having a coordinating role for national cyber-security exercises. One n/g CERT runs a service for citizens that is focused on warning against computer viruses and other malware in computer programs. Nowadays, n/g CERTs are often requested to run or to take part in cyber-security exercises on national level involving critical information infrastructure organisations. There is a new trend emerging where the n/g CERTs invite their peers from neighbouring countries or other Member States to participate in the exercise. These actions tend to foster regional cooperation, while cooperation on a European/global level is enhanced by joint exercises like Cyber Europe.[31]

31 https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe

Figure 11:

Visual scheme of deployment of service portfolio capabilities



n=25 n/g CERTs

Figure 11 provides an overview on deployment of some aspects of the service portfolio capability by Member States. It shows quite a high degree (73%) of satisfaction among constituents with services provided by n/g CERTs. This is also reflected in the fact that nine out of ten n/g CERTs provide education and training to their constituents. On the other hand, less than half of n/g CERTs are involved in business continuity management and disaster recovery planning for CIIP.

4.3.1.1 Constituencies for national/governmental CERTs

The constituency or the customer base of an n/g CERT should in theory consist of all the entities within the state borders (i.e. the full national domains), because any such entity is a potential customer of n/g CERTs. In the case of CERT-EU,[32] the constituency consists of EU institutions.

A generally clear pattern across the Member States was observed based on research conducted: N/g CERTs' constituencies include practically all the entities within the state border, while public and government bodies receive prioritised treatment. In this respect, it is important to stress that a national CERT often also acts as a governmental CERT until new arrangements in the form of a law or strategy are developed. In countries like Poland, Spain, Switzerland or the United Kingdom, there are separate CERTs for both national and governmental constituencies.

32 http://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html

CII providers are also entitled to receive services from the n/g CERT, However, they can also use their own teams that are charged with handling security incidents, so n/g CERTs are supposed to play a more supporting role. This might be important especially in cases when the n/g CERT lacks the sector-specific knowledge (i.e. ICS, SCADA).[33]

CERTs with a background in research and educational network institutions that have become the *de facto n/g CERT continue to serve their original constituencies. Other stakeholders usually receive only a subset of services and ordinary citizens are advised to first contact their ISPs when they believe that they (their computers) have been a victim of a cyber-attack.*

4.3.1.2 Incident handling and other reactive services

Incident handling, analysis and response coordination (grouped under the term of incident management), is the core service of each n/g CERT that it must provide to its constituents. This is still the case even though n/g CERTs now tend to increasingly focus on proactive services.

Reactive services include the four basic categories:

- Alerts and warnings
- Incident handling
- Vulnerability handling
- Artifact handling

The more mature the n/g CERT is, the more reactive services it tends to provide to its constituents. One example of this is artifact handling capability, which is still not universal among n/g CERTs. One n/g CERT that does not provide artifact handling capabilities explicitly stated that such a service is not supposed to be provided under its current mandate.

On the other hand, in countries with extensive national networks of CERT communities (e.g. the United Kingdom and Germany), the n/g CERTs offer the full range of reactive services. These n/g CERTs are part of the national cyber-security centres or similar institutions and are sufficiently staffed and equipped to deliver not only reactive services, but also proactive and security quality management services.

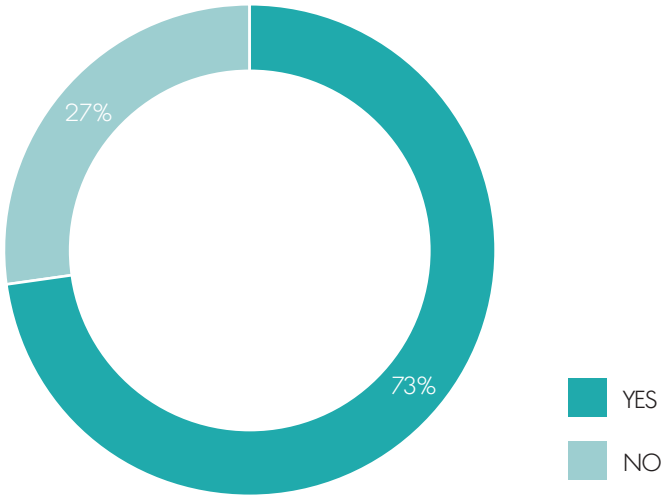
N/g CERTs universally report providing alerts and warning services. They collect information about ongoing security incidents either automatically (collected from sensor systems, honeypots, darknets and other such systems) or through information provided by third parties such as other CERTs.[34] The alerts include an assessment of the threat and advice for further action (patches to apply, software to avoid, ports to block at the firewall level, etc.).

33 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states

34 ENISA carried out a study on proactive detection of incidents: http://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-report

When assessing the deployment of incident handling capabilities, it is especially important to examine the opinions of constituents regarding their overall satisfaction with the services provided by n/g CERTs (see Figure 12). Telecommunication operators and government institutions in general regard the activities of n/g CERTs positively (not just in the area of incident handling). One of their opinions is illustrative: 'Despite a lack of empowerment from the government institutions there is a good coordination effort and a very good sense or responsibility and coordination between the members.'

Figure 12:
Satisfaction of constituents with services provided by n/g CERTs



n=11 other stakeholders (other than n/g CERTs)

Because incident handling often requires international coordination, there is a significant need for standardised formats to exchange incident data (and also a standardised list of incident types). Most n/g CERTs interviewed are in favour of this idea and would support it at the international level. On the contrary, one n/g CERT is of the opinion that no standardisation is necessary or even realistic in the short term, although it also acknowledges the need for a certain level of expectations about what information the probable exchange formats should include.

4.3.1.3 Proactive services

Proactive services offered by n/g CERTs aim to reduce the number of cyber-security incidents by implementing preventive measures. These services include:

- Announcements;
- Technology watches;
- Security audits and assessments;
- Configuration and maintenance of security tools, applications, infrastructures and services;
- Development of security tools;
- Intrusion detection services;
- Security-related information dissemination.

4.3.1.3 Proactive services

The increasing focus on proactive services is reflected in the way that n/g CERTs deploy these services. It is now common for n/g CERTs to publish advisories for events and incidents that are considered to be of special importance to its constituents. Information is disseminated via various channels including new social media (web, mailing lists, RSS feeds, Twitter feed) depending on the type of information.

With security-related information dissemination, n/g CERTs now provide constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security.[35] Such information might include reporting guidelines and contact information for the n/g CERT, archives of alerts, warnings and other announcements, documentation about current best practices, and last but not least, current statistics and trends in incident reporting.

The provision of statistics on incidents is becoming a sought-after service among constituents and is a good source for tracking the activities and success rates of n/g CERTs in incident handling. N/g CERTs release or, in the case of newly established teams, plan to release statistics on a regular basis. However, statistics will not be made public in all cases. The website of the n/g CERT in the Czech Republic provides an example of well-structured and constantly updated statistics on incidents (going back several years).[36]

It is interesting that some constituents believe that the scope of proactive services is becoming too big for an n/g CERT to handle. One respondent specifically referred to duplicative work that is being done by disseminating information on proactive announcements or technology watches by several CERTs and vendors. This respondent says that this service is nowadays readily available on the Internet so that it is not useful to waste the valuable resources of n/g CERTs on such services.

"As the definition of national cyber-security and critical information infrastructure is vast, we recommend allowing CERTs to proactively scan online infrastructure to detect unprotected infrastructure. In that scope, it would be necessary to improve the laws to allow CERTs to do such scanning on the Internet and report the vulnerabilities to the owner."

n/g CERT respondent

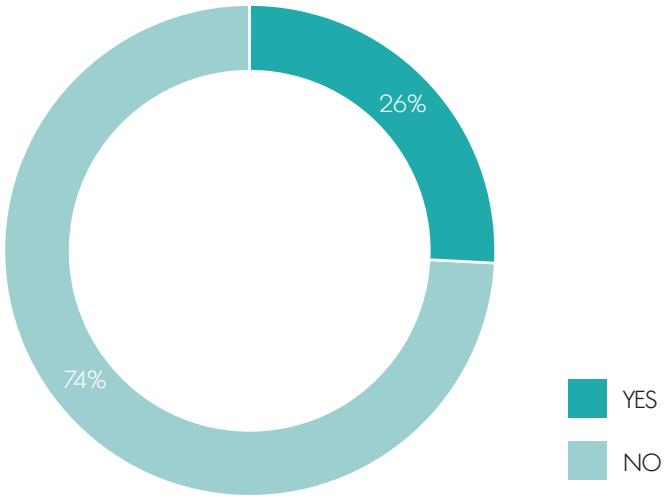
35 http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder

36 http://www.csirt.cz/files/csirt/statistics/stats.html

4.3.1.4 Services provided beyond basic scope

Although the current service portfolios of n/g CERTs are considered to be appropriate (see section 4.3.1.8) by most n/g CERTs and their constituents, n/g CERTs also provide activities requested by their constituents. The n/g CERTs themselves classify these activities as 'new' within the typical CERT service portfolio and more than a quarter of n/g CERTs report to deliver such services (see Figure 13).

Figure 13:
Services considered 'new' within typical CERT portfolio



n=23 n/g CERTs

One n/g CERT developed extensive vulnerability coordination services,[37] while other n/g CERTs provide legal support to their constituencies. A good example of an n/g CERT providing innovative services is one n/g CERT developing its own tools in the area of proactive detection and incident handling. Their research activities in this area allow them to operate as an analysis centre for cyber-security incidents in their country.

The 'new' services of n/g CERTs can also be classified according to services which were requested by public institutions or CII organisations. Examples include running an awareness raising project financed by the Ministry of Education or acting in a coordinating role for the national cyber-security exercises. One operator reported as an additional service organising working groups on specific topics in the area of cyber-security. The n/g CERT in Germany runs a service (Bürger-CERT)[38] for citizens which is focused on providing warnings against computer viruses and other malware in computer programs.

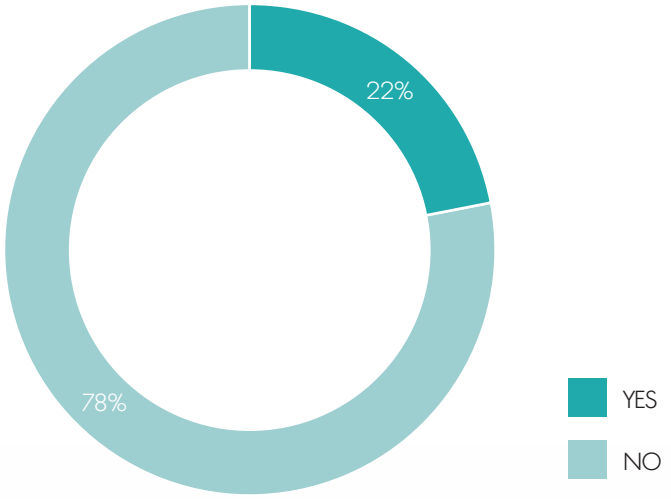
37 http://www.cert.fi/en/activities/Vulncoord.html

38 https://www.buerger-cert.de/

4.3.1.5 Outsourcing

Incident Management and Alerts & Warning are definitely services that the n/g CERT should provide. For other services, n/g CERTs can consider outsourcing some of their less immediate, mid- and long-term services. Less than one-quarter of n/g CERTs use outsourcing services to some extent (see Figure 14).

Figure 14:
Use of outsourcing by n/g CERTs



n=23 n/g CERTs

Among the services that n/g CERTs outsource to third parties are the following:

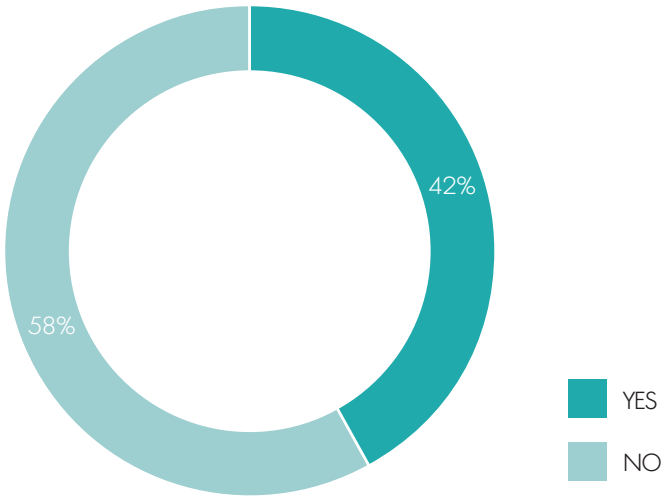
- event coordination
- legal services
- software development
- writing of security advisories for public institutions
- sensor and data/information acquisitions.

4.3.1.6 Involvement in Disaster Recovery Planning and Business Continuity Management for CIIP

Disaster Recovery Planning (DRP) and Business Continuity Management (BCM) is a key aspect of national plans for critical information infrastructure protection. These services are an important component of security quality management services, as n/g CERTs providing these services can use and aggregate the output of both the proactive and reactive services.

Only about 40% of n/g CERTs reported that they are involved in DRP and BCM (see Figure 15). The level of involvement varies based on the mandate and relations with the hosting organisations. One NRA hosting an n/g CERT has developed a series of regulations in this area, which helps the n/g CERTs to be active in DRP for CIIP. Other n/g CERTs are involved directly or are consulted occasionally by the responsible entities.

Figure 15:
Involvement in DRP and BCM for Critical Information Infrastructure Protection



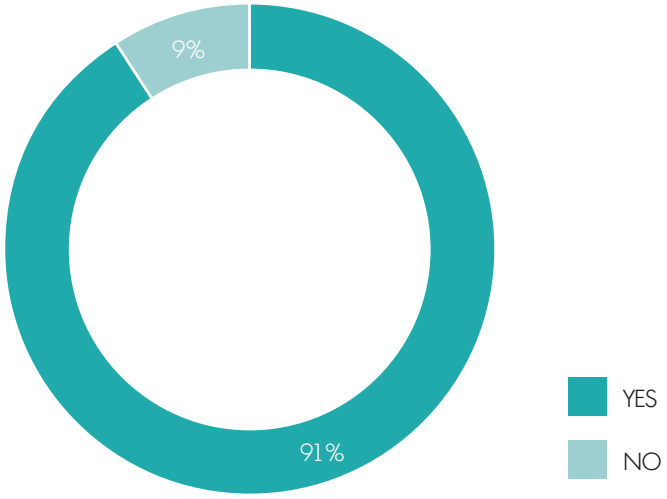
n=24 n/g CERTs

The involvement of n/g CERTs also relates to improving awareness, establishing information sharing mechanisms with operators, assessing risks and developing structured exercises. As two n/g CERTs suggested, the addition of this capability will probably follow more often with the adoption of new national cyber-security strategies.

4.3.1.7 Educational and training services

Depending on available resources, n/g CERTs often undertake advanced education and training on best practices in cyber-security for their constituents. The services mentioned also belong to the type of security quality management services that n/g CERTs are very well placed to provide due to their in-house cyber-security expertise. In the survey, around 90% of n/g CERTs indicated they provide various forms of educational and training services (See Figure 16).

Figure 16:
Educating constituents on best practices in cyber-security



n=22 n/g CERTs

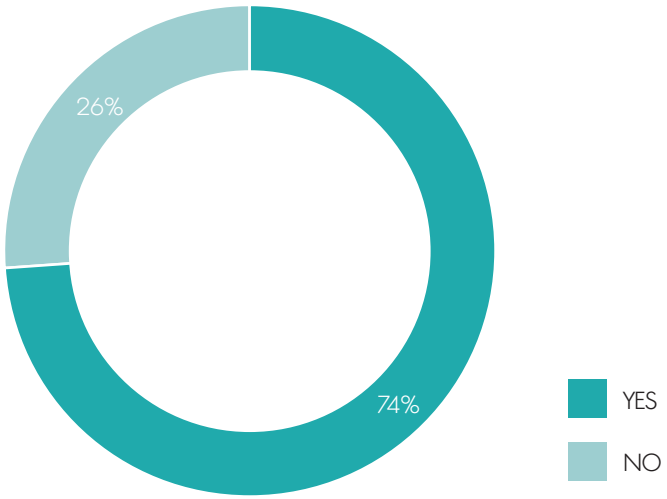
The training services provided include conferences, workshops, courses, tutorials and to an increasing extent holding national exercises. Approximately half of n/g CERTs organise or take part in national cyber-security exercises. The frequency of these services and the types of educational activities offered are based on the requests of constituents, and may be included in contracts with constituents. In one interview, an n/g CERT highlighted its role as an educator of LEAs in the area of cyber-security issues.

As for national cyber exercises, n/g CERTs that provide them on a national level involving critical information infrastructure organisations usually do so once a year or every two years, while more mature and resourceful n/g CERTs may carry them out several times a year. One n/g CERT commented that it was expecting a grant this year to go ahead with its national exercises. A new trend has emerged and become quite popular in which n/g CERTs invite their peers from neighbouring countries to such exercises. This tends to foster regional cooperation, while the cooperation on European/global level is enhanced by joint exercises like Cyber Europe or NATO exercises, among others.

4.3.1.8 Sustainability of current scope of services

The evolving security landscape and the assessment of deployment of current baseline capabilities raises the question of whether the service portfolio as included in the original Baseline Capabilities document and/or a CERT/CC document 'Handbook for CSIRT', which ENISA is using as a source of reference, is still adequate.[39] Almost three-quarters of n/g CERTs agree that the service portfolio table of CERT/CC still reflects the actual services that n/g CERTs provide, even though it was first published in 1998 and updated in 2003 (See Figure 17).

Figure 17:
Current scope of services considered relevant



n=19 n/g CERTs

A number of n/g CERTs are calling for more significant involvement with regard to legal issues and cooperation with LEAs on fighting cybercrime. One interviewed n/g CERT indicated that there is a need for a more straightforward approach when dealing with law enforcement agencies, and that n/g CERTs should be able to resolve some issues (e.g. spam) on their own without involving the police. A sentiment echoed throughout the survey (not just for service portfolio capability) was that the legal competence of n/g CERTs is becoming crucial, although technical competence remains the key factor.

According to one n/g CERT that elaborated on this topic in detail, the service portfolio itself is still relevant. However, it is becoming more a question of a shift of focus and how it is portrayed to the outside. N/g CERTs need to reinvent themselves constantly by delivering their own advanced analyses instead of merely repeating information obtained from other sources. It is also important that n/g CERTs manage this shift without excessive organisational/managerial overhead. Thus far, n/g CERTs have found that organisational/political issues can become a contentious issue when trying to carry out this shift.

Clarifying definitions of the items of service portfolio was mentioned as an issue by a few n/g CERTs, as they were not sure whether some services are included in the portfolio. One example of this is situation awareness, and one respondent questioned whether services commonly provided by n/g CERTs like malware/software analysis and reverse engineering fall under artifact analysis or under another category.

39 http://www.enisa.europa.eu/activities/cert/support/guide/strategy/services Please note that under the CERT/CC scheme of services, artifact handling capacity is treated as a separate service rather than being part of the group of reactive services.

4.3.1.8 Sustainability of current scope of services

The constituents of n/g CERTs referred to the need for improving the provision of existing services or even launching services from the current portfolio instead of naming new services that they would like to see launched. Operators called for more detailed advisories and generally services regarding telecommunication networks. A few other CERTs voiced concerns that the n/g CERTs (especially those with the governmental role) do not make certain relevant information available.

Conclusions

All core services of n/g CERTs are provided to their constituents. However, only more mature n/g CERTs are able to cover the complete broad portfolio of services. For example, some n/g CERTs do not provide artifact or vulnerability handling. In order to streamline incident handling internationally, the teams are in favour of developing standardised formats for information exchange. Regarding proactive services, the teams provide a wide range of services and they use multiple platforms for communicating them, including popular social media. The n/g CERTs have made significant progress in educating their constituents on cyber-security topics as nearly 90% of them organise workshops or seminars or participate in working groups. On the other hand, still only a minority of the teams are involved in disaster recovery planning and business continuity management for CIIP.

The current service portfolio for n/g CERTs remains valid; however, there should be adjustments reflecting the evolving cyber-security landscape. This is especially the case with regard to cooperation with LEAs on cybercrime. The legal competencies of n/g CERTs are becoming more important, although their level of technical competence remains paramount. N/g CERTs need to reinvent themselves constantly by delivering their own advanced analyses instead of merely repeating information obtained from other sources.

Regarding the service portfolio capability, a number of deployment shortcomings/gaps have been identified, which are further addressed in the accompanying report 'Baseline Capabilities of national/governmental CERTs – Updated Recommendations 2012'.

Key shortcomings include:

- When handling incidents internationally, the partnering n/g CERTs often do not act in accordance with the information provided, which supports the need for standardised formats in information exchange.
- Vulnerability and artifact handling are not provided by all n/g CERTs.
- N/g CERTs do not often develop their own tools.
- The general statistics on incidents are still not universally made public by n/g CERTs.
- Provision of some of the proactive services, like technology watch, may be redundant.
- The majority of the n/g CERTs are not involved in disaster recovery planning and business continuity planning for CIIP.[40]

40 Research did not distinguish between private and public sector disaster recovery planning and business continuity management for CIIP.

4.4 Operational Capabilities

4.4.1 Overview

Operational capabilities of n/g CERTs relate to four main areas – human resources, infrastructure, service delivery and business continuity. Although factors such as mandate, regulatory measures, size of the country and business hours are all instrumental in determining the size of the n/g CERTs, for the European environment a 6–8 member team is generally considered to be capable of providing an acceptable level of service[41]. In most Member States, n/g CERTs have staffs with more than 8 FTEs, and there are also cases where the number is three times as high. However, some n/g CERTs operate with only four to five staff. Nevertheless, special care should be taken when interpreting these figures as n/g CERTs are frequently supported in an ad hoc fashion by personnel of the hosting organisations. Some n/g CERTs publish contact details (or even photographs) of individual team members on their websites, while others show only general email addresses.

On the other hand, there are no major differences (at least in theory) regarding the need to provide multiple means of reaching n/g CERTs, which is *de facto* the rule for all n/g CERTs. The same holds true for security requests, where PGP-encrypted emails are the most commonly used, as are various classification schemes for incidents. While some n/g CERTs provide templates or guides for submitting incident reports (e.g. Belgium, Bulgaria, Malta, Spain) based on international best practices, more Member States still seem to not use fixed forms.

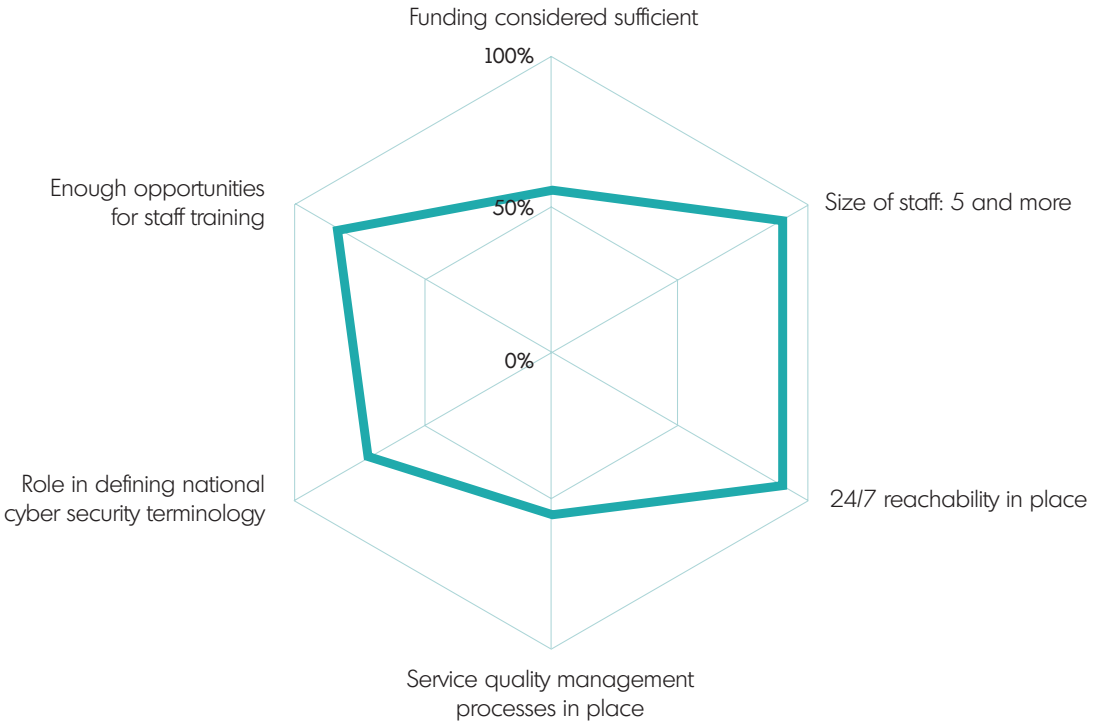
In order to ensure service delivery and business continuity, n/g CERTs preferably demonstrate the capability to react to incidents on a 24/7 basis. In the vast majority of cases, the n/g CERTs are able to manage this. Although they routinely operate in normal business hours and sometimes lack sufficient resources, on-call duty and at least basic outside monitoring of emails is ensured. However, this facility is not always stated clearly on the n/g CERTs' websites.

Many n/g CERTs still complain about a lack of funding, especially in the newer Member States of the EU, which does not allow them to provide additional services. The funding usually comes from the government and hosting organisations. Where n/g CERTs are hosted by NRAs, a part of the budget flows directly from the operators in the form of a small portion of their yearly turnover.

41 As stipulated in the previous version of Baseline Capabilities document

4.4.1 Overview

Figure 18:
Visual scheme of deployment of operational capabilities



n=25 n/g CERTs

Figure 18 provides an overview on deployment of some aspects of operational capabilities by Member States. While the majority of n/g CERTs (85%) have 5 staff and more and plan to further increase staff numbers, they face funding constraints as only 55% of CERTs consider the amount of funds to be sufficient. The teams also take measures to have their staff appropriately trained and nearly 80% of n/g CERTs believe that there are enough opportunities for training of staff. Less than 60% of n/g CERTs have service quality management in place. But nearly 90% of them are reachable on a 24/7 basis and those n/g CERTs who do not yet display this functionality are planning to do so when they have completed their set-up phase.

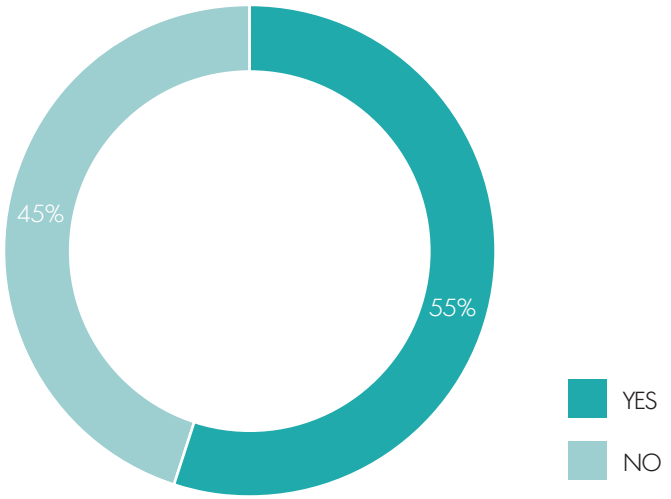
"Generally speaking, the organisations and teams with mature incident handling processes and outward-facing points of contact are the easiest to work with regardless of where they come from geographically."

n/g CERT respondent

4.4.1.1 Funding model

In order to be able to provide high value services to their constituents, n/g CERTS have to be allocated sufficient financial resources for staff and equipment. In this regard it seems that the situation is improving as new strategies and mandates envisage an enhanced role for the n/g CERTs, which should also result in increased funding. A slight majority of n/g CERTs that commented on this topic believe that the current level of funding is sufficient for them to fulfil their expected tasks (See Figure 19). However, many n/g CERTs still reported a lack of funds, especially in the newer Member States of the EU.

Figure 19:
Funding considered as sufficient



n=11 n/g CERTs

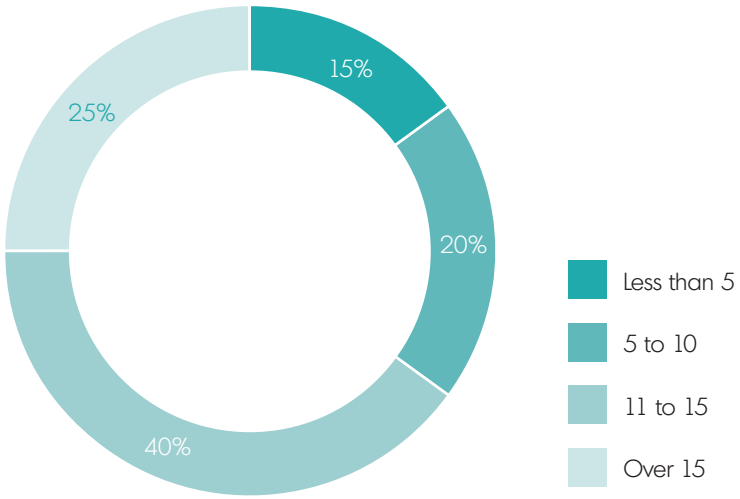
Funding for n/g CERTs usually comes from governmental bodies and hosting organisations. Where n/g CERTs are hosted by NRAs, a part of the budget flows directly from the operators in a form of a small portion of their yearly turnover. But a few n/g CERTs are also actively seeking and generating funds from other sources. These sources relate especially to commercial and research activities, including applications for grants at national and European institutions. In one interesting case, an n/g CERT is funded entirely by the hosting organisation (national TLD administrator – a private company), although the team temporarily acts (acted) as a CERT for the government institutions as well.

The size of a budget does not seem to be directly related to a country's size. For example, one n/g CERT in a smaller Member State indicated that they have a budget of around €2 million. On the other hand, its counterpart from a larger Member State claimed a budget worth €1.5 million. And both are regarded by their peers as more mature n/g CERTs.

4.4.1.2 Size of staff, its composition and responsibilities

The original Baseline Capabilities document suggested that n/g CERTs needed at least six to eight staff members at minimum to provide 24/7 availability for both constituents and their counterparts in other countries. Most n/g CERTs meet with this requirement (see Figure 20). The largest proportion (nearly one-half) of n/g CERTs have staffs of 11 to 15, followed by teams with between 5 to 10 staff. There are also equal groups of n/g CERTs that either have quite large staffs (15 and more) or, on the other hand, work with less than 5 full-time equivalents (FTEs).

Figure 20:
Size of staff on national/governmental CERTs



n=24 n/g CERTs

Caution should be exercised, though, in interpreting these numbers too strictly. In many cases there are other experts (staff within the hosting organisations or hired personnel) working on concrete tasks of the n/g CERTs. Often, administrative and legal tasks are delivered by the hosting organisations as well. The overwhelming majority of n/g CERTs aim to increase (or to a lesser degree at least maintain) the size of their current staff, which a majority of their constituents also support (also 56% of other stakeholders are of the opinion that the number of staff should increase). In one Member State the relevant n/g CERT is faced with a reduction in staff size, on account of the economic and financial crisis affecting the country.

The composition of the teams generally follows the recommendation from the original Baseline Capabilities, in that there is a team leader, several incident handlers and a number of technical experts. Seventy-five percent of other stakeholders claim that the composition of the team is satisfactory. More resourceful n/g CERTs have more specialised experts, for example in the areas of research and development or law. As for allocating staff for the types of services provided by n/g CERTs, it is difficult to provide precise figures as staff members are typically required to carry out multiple tasks. The teams often cite challenges in finding experts with experience; for example, in the areas of digital forensics analysis, artifact and vulnerability handling, programming, system development and legal support. N/g CERTs are trying to attract these people by offering a unique job including possibilities for personal and professional development such as access to latest technologies and networking with high-level experts in other countries. According to n/g CERTs, there is also a problem with IT educational institutions not producing enough experts for practice.

4.4.1.3 Training of staff

N/g CERTs need to ensure that their employees have the appropriate skills and expertise, which implies continuous investment in human resources. N/g CERTs offer their team members enough opportunities for training and education, as long as time and budgetary resources permit. But they also acknowledge that the best training is working for the n/g CERT as this is a unique job position.

New team members are trained by advanced staff and also attend training courses, conferences and workshops, both national and international. Team leaders encourage staff members to participate actively in these events. The most common examples of this type of training include TERENA/TRANSIT and SANS training or ENISA workshops, while n/g CERTs also use seminars organised by specialised IT companies.

Although these courses and seminars are good enough to provide extensive training on general cyber-security topics, especially for the newly established teams, they are regarded by more mature teams as too basic and not going into the needed technical detail. These mature teams face difficulties in finding high-quality training nationally (e.g. for software reverse engineering service), or even in Europe, while they are sometimes available in the US only or in some other countries outside Europe.

"There are a lot of non-technical training courses across Europe but it's quite difficult to find highly specialised technical training in Europe as they usually take place outside Europe."

n/g CERT respondent

4.4.1.4 Communication means and their security

For constituents and parties reporting incidents or for the collaboration partners it is important to know how to contact n/g CERTs. It is now standard for all n/g CERTs with the exception of the newly established ones to operate their own websites (mostly with some sections also available in English), where the contact details are given. They are structured according to information delivered, with incident reporting being prioritised. Email (PGP-protected) is a preferred means of communication, with phone connections also readily available. The use of web forms in websites addresses the wider constituency, giving readily available access to the n/g CERT. Still, specific stakeholders such as governmental bodies and specific CIIP stakeholders often turn to use direct phone lines. N/g CERTs also publish incident reporting forms including those that are https-protected.

The teams' telephone numbers and email addresses are usually published on the n/g CERT's web page. The constituents are periodically instructed on how to get in contact with the n/g CERT and report incidents. The constituents also receive information on contact details via personal meetings, official letters, presentations at workshops and conferences and other means. Several n/g CERTs have also started to use popular social media like Facebook and Twitter for disseminating less critical or less sensitive information to their constituents. The constituents are generally (in 64% of cases) satisfied with templates provided for reporting incidents but call for data exchange to be more automated.

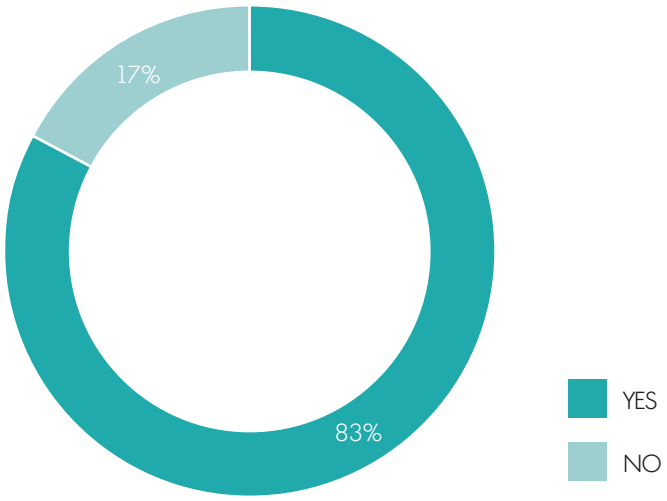
It is interesting to note that some n/g CERTs are being more transparent than others when disclosing the details about team members. While the majority provide basic contact details, a few n/g CERTs in countries with cultures of transparency also publish the contact details (in one case even the photographs) and positions of the team members. But as one n/g CERT said in the interview, the level of openness may change (decrease) if the team is also entrusted with the governmental CERT role.

The security of communication is provided mainly via PGP-encryption and further by means of S-MIME, ACID, CHIASMUS, HTTPS (SSL in general), SSH or cryptographic communication with public institutions. For security reasons, it is also important that communication channels are backed up or made resilient. Not many n/g CERTs were willing to share further information for confidentiality reasons, but those that agreed indicated that they are using more service providers as a back-up solution.

4.4.1.5 24/7 operational capacity

The operational mode based on 24/7/365 availability allows constituents to report incidents at any time. The provision of service on this continual basis increases the level of trust among the constituents. N/g CERTs have achieved real progress in deployment of this capacity. More than 80% of n/g CERTs are able to handle incidents 24 hours a day (see Figure 21). The remaining n/g CERTs are either still in the initial building-up phase or will provide 24/7 capabilities very shortly.

Figure 21:
Staff available out of official working hours



n=24 n/g CERTs

Although regular working hours are approximately between 9:00 and 17:00, support outside these times is possible usually via a hotline (fixed or mobile) and/or remote access. Usually at least one person is on-call duty, but this number reaches up to six persons in case of one n/g CERT. N/g CERTs are often alerted in real-time via linkage to government TETRA networks, and some have tested this facility with DDoS attacks, for example.

4.4.1.6 Physical security measures

As the n/g CERTs may deal with sensitive information that needs to be protected, adequate measures must also be taken to secure the premises of the teams. Processing sensitive information not only within their constituencies but also from other Member States and other countries makes this even more important.

All n/g CERTs take the utmost care that their premises comply with the requirements mentioned above. For these reasons, the level of security is appropriate for organisations dealing with CIIP and these facilities are in some cases classified as NATO/EU secret. The most common practice is that the facilities are guarded on a 24/7 basis by security guards with security access cards mechanisms for entering the building. Within their hosting organisations, the teams may even have separate access doors. In one case an n/g CERT specifically indicated that visitors are not allowed to use any private devices within the team's premises.

The level of attention that n/g CERTs pay to security measures in their premises is evidenced by the reluctance of the teams to give any details on this topic. However, it is interesting to note that despite these proclaimed security arrangements, two operators believed that the physical security measures are somewhat lower than those for a typical data centre or network operation centre.

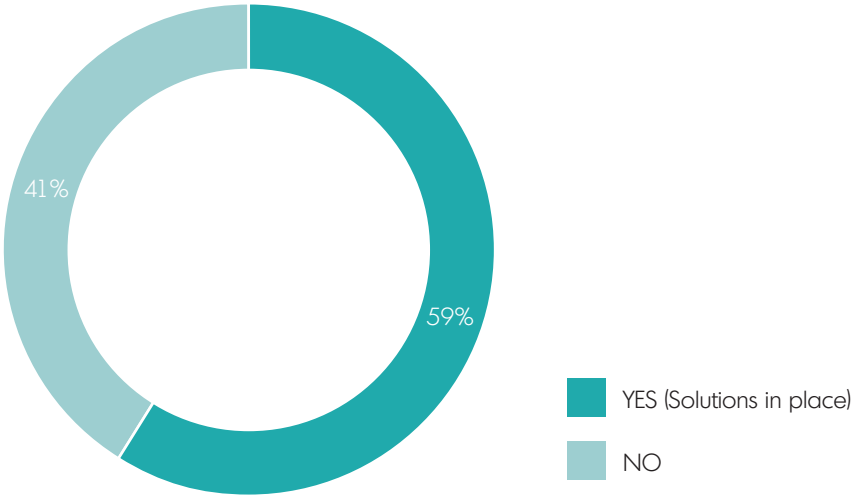
4.4.1.7 Information quality standards and service management improvement processes

N/g CERTs need to have in place a service quality management system to follow up on performance to ensure continuous improvement in processes. This involves development and subsequent monitoring of the most important key performance indicators (KPIs). These KPIs should be relevant to the key mission objectives of the n/g CERTs that are stated, e.g. in the RFC 2350 documents.

Web research conducted for this report revealed that although RFC documents are published by the majority of CERTs on their website, a significant portion of n/g CERTs still do not seem to display RFC documents.

Less than 60% of the teams have certain service management processes (see Figure 22), which most often relate to ISO-27001 and ISO-9001 certificates, but also adhere to standards like the CVE scheme for vulnerabilities and other norms. The Traffic Light Protocol (TLP) has proven to be a useful generic guideline on information sharing. If the teams are not certified in any particular information security quality standard, they draw on experience, 'four-eyes' check policy on official communication and other internal quality controls including terminology. An indispensable tool for incident management service is an incident recording and tracking system (ticketing system), and n/g CERTs are using mainly OTRS, RTIR or Abuse Helper.

Figure 22:
Service quality management in place



n=22 n/g CERTs

4.4.1.8 Best Practices and n/g CERTs' role in dissemination of terminology

Building their own KPIs and service quality management processes are closely linked for n/g CERTs with identifying, adapting and applying best practices learned from their peers and CERT associations. These best practices relate to incident reporting forms, information classification schemes and all the issues of priority and feedback. As to sources for best practices, most n/g CERTs cite ENISA documents and the CERT/CC association, which gathers more mature n/g CERTs. In addition, other sources are mentioned in this respect, including OECD, the SANS Institute or US NIST special publications.

The lessons learned and skills and expertise acquired can then be used by n/g CERTs in the dissemination and definition of terminology for use within the cyber-security community domestically. More than two-thirds of n/g CERTs claim to exercise such a role at national level, either formally or informally. They may be either instrumental in preparing glossaries of terms or have the role of technical advisor in working groups established for these purposes.

4.4.1.8 Best Practices and n/g CERTs' role in dissemination of terminology

Conclusions

The staff of n/g CERTs in 85% of cases consist of at least five FTEs, which is enough for provision of a basic level of continuous service. At the same time they are planning to increase their staff levels, which is also in line with requests of constituents.

However, the teams face the challenge of funding restrictions, which prevent a significant increase in investments. But they still devote resources to train their staff adequately, especially because it is often necessary for the staff members to perform various technical tasks. Availability outside working hours is reported by a vast majority of n/g CERTs, while the remaining newly established n/g CERTs plan to introduce it shortly. Sufficient security measures are taken to protect the premises of the teams. The n/g CERTs also provide various communication channels in case some channels fail. On the other hand, some 40% of n/g CERTs do not have any service quality management processes in place.

Regarding the operational capability, a number of deployment shortcomings/gaps have been identified, which are further addressed in the accompanying report 'Baseline Capabilities of national/governmental CERTs – Updated Recommendations 2012'.

Key gaps include:

- The n/g CERTs rely on state funding and are not active enough in looking for additional resources.
- Legal and PR experts are missing among the staff of n/g CERTs.
- The teams also face difficulty in recruiting highly specialised personnel, for example in areas of reverse engineering or digital forensics.
- There are not many opportunities in Europe for training in deep technical aspects.
- Although the teams mostly provide their core services on a 24/7 basis, this functionality is not often displayed on the n/g CERTs' websites.
- Constituents are satisfied with templates provided for reporting incidents but call for data exchange to be more automated.

4.5 Cooperation

4.5.1 Overview

Due to the global nature of cyber-security it is crucial that the n/g CERTs establish as many working relationships with other stakeholders in the CIIP area as possible. N/g CERTs are all working towards achieving this goal; however, they still face various difficulties. It is important that the roles of n/g CERTs are clearly stated in the mandate, so that the unnecessary competition between domestic CERTs is avoided (such cases were reported from two countries). On the other hand, in many countries there are no such problems and the cooperation of domestic CERTs with clear coordinating roles of n/g CERTs is well formalised.

As regards cooperation with CII operators and other operators and service providers, the structures seem to be in place and generally working properly to the satisfaction of constituents. It is a common feature that the n/g CERT's recommendations cannot be enforced and that the constituents may act upon them only voluntarily. As the n/g CERTs need to work closely with law enforcement agencies (LEAs) on cybercrime issues, they are starting to develop cooperative relations with these bodies. This kind of cooperation tends to be one-sided, however, as LEAs have limits on sharing information until the relevant investigations are over.

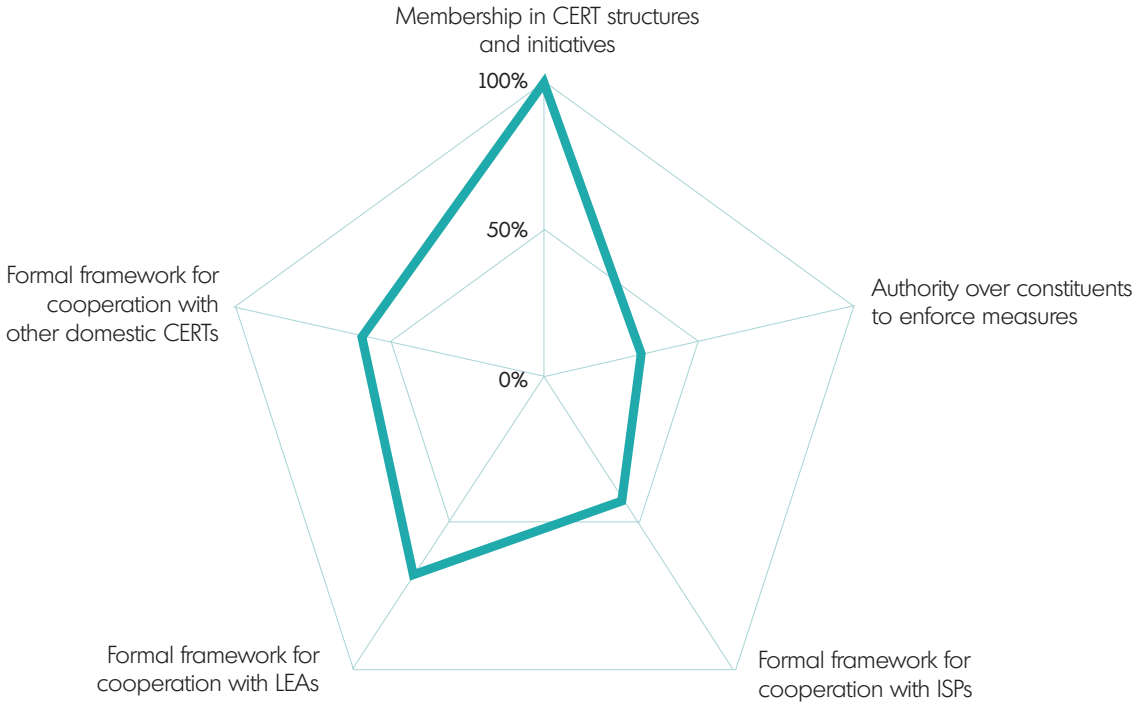
The Netherlands, for example (partly thanks to the incorporation of GOVCERT.NL into the newly created National Cyber-security Centre) has built effective arrangements for the cooperation of the n/g CERT with other stakeholders. This is evidenced by symposia that the team hosts and that are widely appreciated by constituents and cooperation partners.

A lot of work has been done in international cooperation and presence of n/g CERTs, as it is indispensable for cross-border incident handling. N/g CERTs in EU Member States actively engage in respective international and European forums such as FIRST, TF-CSIRT, Trusted Introducer and several ENISA initiatives. Accompanying membership processes are necessary for the n/g CERTs to be considered trustworthy by their peers.

4.5.1 Overview

Figure 23:

Visual scheme of deployment of cooperation capabilities



n=25 n/g CERTs

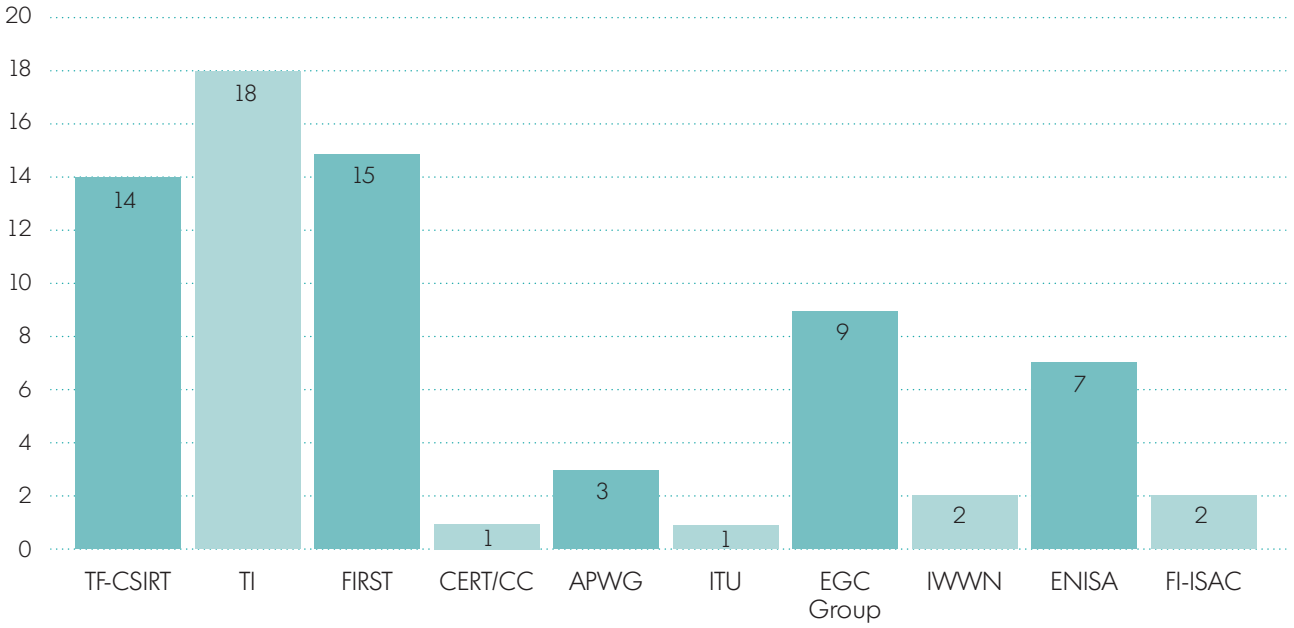
Figure 23 provides an overview on deployment of some aspects of the cooperation capabilities by Member States. While all n/g CERTs are embedded in the European or international CERT associations (or the newly established teams are heading in this direction), frameworks for cooperation with domestic partners are less formalised. Most often there are formal agreements with LEAs, while with other domestic CERTs the cooperation is based on a formal framework only in 58% of cases and with ISPs only in 42% of cases. Some degree of authority (usually through the hosting organisation) over the constituents to enforce measures is reported by only about 30% of n/g CERTs.

4.5.1.1 Membership in CERT structures and initiatives

Membership in various CERT initiatives is widespread throughout the EU. With a couple of exceptions, all n/g CERTs indicated that they are members of one or more of them. The most common structures that n/g CERTs belong to are Trusted Introducer,[42] FIRST[43] and TF-CSIRT.[44] Other popular structures included EGC Group,[45] ENISA's workshops and working groups[46] and the Anti-Phishing Working Group.[47] Feedback on the value of cooperation and information sharing in these initiatives varied greatly depending on the type of organisation in question. Respondents tended to compare international organisations in terms of their value as a platform for networking versus as a platform to exchange more technical knowledge and experiences. They are seen as being valuable for meeting others in the security community. Some respondents, however, indicated that in some cases these structures could do more in terms of offering technical platforms for sharing incidents or artifacts in real time.

Figure 24:

Respondents' membership in international CERT initiatives*



n=21 n/g CERTs

*Quoted spontaneously. Respondents were not given a specific list of organisations and may belong to other initiatives.

42 https://www.trusted-introducer.org/teams/country_LICSA.html
43 http://www.first.org/
44 http://www.terena.org/activities/tf-csirt/
45 http://www.egc-group.org/
46 http://www.enisa.europa.eu/activities/cert/events
47 http://www.antiphishing.org/

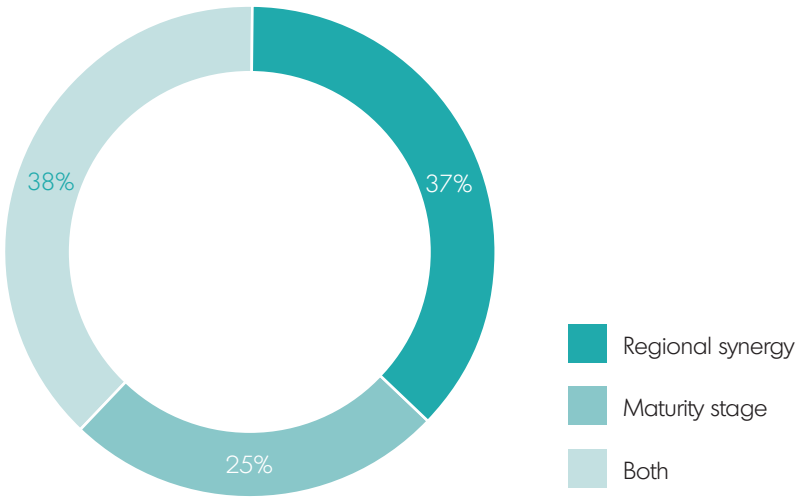
4.5.1.2 Bilateral cooperation

Aside from participating in various CERT- and other security-related initiatives, n/g CERTs are taking it upon themselves to coordinate directly with other n/g CERTs in Europe and globally, driven by shared interests in addressing certain operational tasks (sharing of knowledge and expertise) as well as dealing with more immediate security-related initiatives that are relevant to their specific geographic location. Such instances of bilateral coordination within Europe are often on a regional level, for example throughout Benelux or throughout Scandinavia, as well as between two or three countries that share a common border.

In many cases cooperation is driven by an immediate need that arises, for example a specific security threat. In other cases there are regular meetings and ongoing exchanges of information, typically conducted over email, telephone, at conferences, on-site visits and real-time messaging platforms. The nature of this coordination is typically informal, particularly in cases where n/g CERTs want to exchange experiences and best practices. Otherwise, Memorandums of Understanding as a type of formal agreement are common. There are instances of n/g CERTs forming legal agreements, typically Non-Disclosure Agreements, with n/g CERTs in other countries, in cases where operational cooperation is required. But feedback indicates that formalising a cross-border legal agreement can be challenging, and there are concerns that a formal legal agreement could actual inhibit the cooperation. Consequently there is a preference to keep the cooperation informal where possible or rely more on MoUs. Two key factors supporting cooperation with n/g CERTs in other EU Member States included regional synergies, and also the maturity level of the other n/g CERT (see Figure 25).

Figure 25:

Factors supporting cooperation with n/g CERTs in other Member States



n=16 n/g CERTs

4.5.1.3 Trust criteria for cooperation with n/g CERTs

CERT cooperation is based on trust. Without trust, n/g CERTs will be less willing to share information and less open to working together on incident responses and handling when needed. Measuring trust and defining criteria by which to measure an n/g CERT's trustworthiness is an ongoing challenge, particularly when the aim of the cooperation is to exchange and share sensitive information. With this in mind, ENISA surveyed respondents to identify the characteristics that they consider as a foundation for building a trusting relationship. Key criteria that n/g CERTs look for includes:

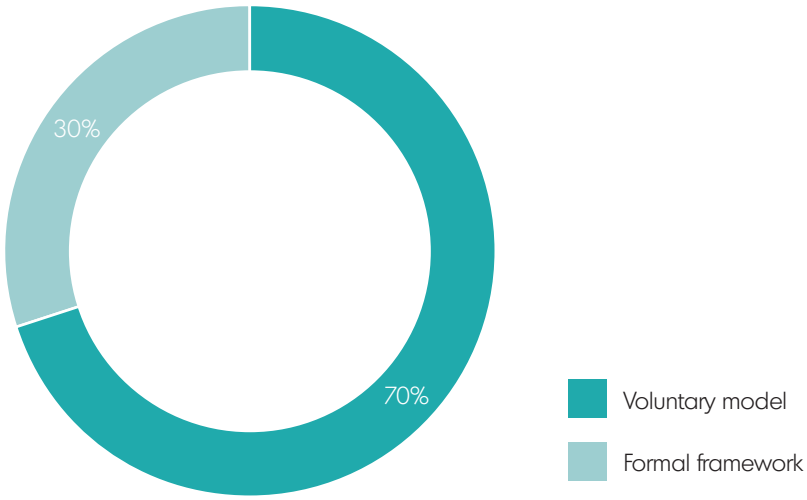
- technical expertise with a proven track record,
- membership in CERT initiatives,
- ability to respond quickly and act on security threats,
- a stable team.

Close relationship with the government was also cited as an important factor. Additionally, n/g CERTs indicated that they take into account what stage the n/g CERT has reached on the maturity index. It is viewed as important that they be at least at the same level, if not higher.

4.5.1.4 Enforcement powers

N/g CERTs continue to have little authority over their wider constituencies in terms of getting stakeholders to implement specific security measures. Out of the n/g CERTs surveyed by ENISA, roughly 30% indicated that they have some authority to require constituents to implement cyber-security measures (see Figure 26). There are cases of some countries preparing to formalise enforcement powers in legislation, but this is still in the early stages. In the vast majority of cases the relationship is voluntary and informal, although it has become common that certain constituents will voluntarily enter into formal, written agreements that specify certain areas for cooperation. These may, for example, take the form of a code of conduct-type document on mitigation of major types of incidents, to which the respective constituents adhere regarding security measures in their networks.

Figure 26:
Authority over constituents to enforce measures



n=23 n/g CERTs

As with the wider constituency, the relationship between n/g CERTs and telco operators and ISPs specifically is typically voluntary, although there are cases where they have signed written agreements which clarify specific areas where they will cooperate. For example, one respondent indicated that it has an agreement with service providers for proactive monitoring service. In other cases, the relationship remains purely informal. In such situations the n/g CERT will have irregular meetings and discussions with the telecommunication operators and ISPs, but the overall trend is that the relationships are built on an ad hoc basis.

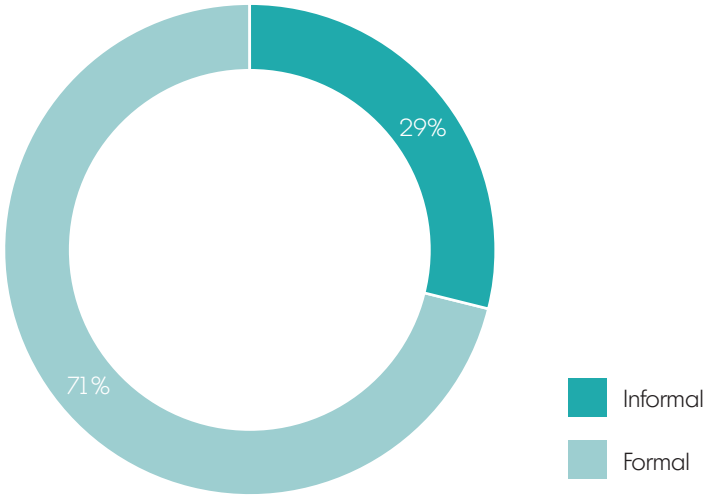
4.5.1.5 Cooperation with law enforcement authorities

Sharing of information (on incidents) between n/g CERTs and LEAs can be critical in addressing security threats. Information collected by n/g CERTs during monitoring exercises can assist LEAs in investigations. Alternatively, LEAs could uncover information during criminal investigations that would assist n/g CERTs in their incident handling and response efforts. Additionally, as most n/g CERTs do not have the authority to implement or enforce certain security measures, they often depend on LEAs for enforcement. For example, if an n/g CERT identifies a malicious server, the details could be passed on to LEAs to launch an investigation and potentially shut it down. Consequently, open lines of communication based on trusted channels are needed to facilitate the cooperation.

The survey of n/g CERTs found that the vast majority of n/g CERTs are cooperating with domestic LEAs, both police and national security, and rate the relationship as being positive. Cooperation between n/g CERTs and law enforcement authorities in more than 70% of cases is based on formal, written agreements (see Figure 27). For comparison, this level is substantially higher than for other domestic CERTs and ISPs, which have such a formalised structure for cooperation only in 58% and 42% of cases respectively.

Figure 27:

Framework for cooperation with law enforcement authorities



n=17 n/g CERTs

In instances when the relationship is informal, n/g CERTs and LEAs still engage in seminars and workshops, where CERTs can share knowledge and expertise. While overall feedback indicated positive relationships between domestic LEAs and n/g CERTs, a few exceptions were noted. In one case, a CERT indicated that the relationship can sometimes be unidirectional. This could be due to legal conditions. Law enforcement officials do not share information about an investigation until the investigation is closed. Under such circumstances, any valuable information that could be shared is withheld by LEAs until the case is closed and as a result can be out of date for n/g CERTs.

Survey results indicate that cooperation with international LEAs is negligible. N/g CERTs in general did not indicate that any formal or informal relationship with international LEAs was in place. In one instance, an n/g CERT did indicate that there were only sporadic discussions with international LEAs and only at a national level.

4.5.1.6 Working groups and associations for domestic stakeholders

Nearly 60% of n/g CERTs indicated that they operate a working group or another type of umbrella activity that brings together members of the cyber-security community for regular meetings to exchange information and expertise. In some cases the working groups bring together other CERTs within the country, while other n/g CERTs open the working groups to a wide cross-section of organisations relevant to cyber-security such as ISPs, academic institutions, public administration, law enforcement authorities, content providers, representatives from the banking sector, other CIIP organisations and ICT experts. In a small number of cases, representatives of the intelligence and military were also involved in such groups. Working groups typically meet two or three times a year, while ENISA did come across one group that maintains a year-round real-time chat room that allows group members to communicate on urgent matters. Overall, more than half of other stakeholders reported taking part in the initiatives organised by the n/g CERT in their country.

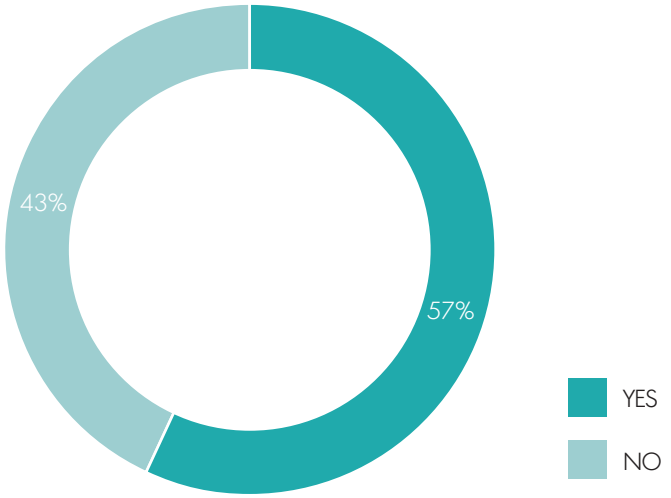
The purpose of the working groups tends to be to enable an open forum for the exchange of ideas, an opportunity to develop standards, set expectations, and discuss threats and incidents' evolution and, last but not least, build trust among the participants. Nonetheless, respondents did give examples of problems that inhibit the working groups from reaching their full potential. Respondents indicated that data protection laws prevent members of the working groups from sharing data that would be necessary for deeper analysis of incidents. Working group members from the private sector, in particular, are cautious about what information can be shared. This ultimately holds the groups back from engaging in more practical exercises during their meetings. Lack of trust is also an inhibitor for groups that include stakeholders from outside the CERT community. Participants can be less open to sharing information or experience when they are in the presence of competitors from the same sector.

4.5.1.7 Special requirements for CII bodies

N/g CERTs oversee a constituency that consists of a variety of organisations with varied implementations of ICT infrastructure and solutions, ranging from telecom operators with nationwide publicly accessible communications networks, to large businesses with multinational private networks. The incident response and monitoring needs consequently vary depending on the nature of the network and technology employed. With this in mind, n/g CERTs face the challenge of positioning their services to address the varied needs of their constituencies. Applying different requirements in terms of incident response, handling and monitoring based on the type of constituent could help n/g CERTs to streamline their activities.

Figure 28:

Need for special requirements for CII operators



n=14 n/g CERTs

At the same time, it might create situations where certain types of organisations receive a higher level of attention, at the expense of others, given an n/g CERT's limited resources. Opinions on this issue vary across Europe. While there is no consensus, a higher number of n/g CERTs believe that obligations and requirements should vary depending on how critical the organisation's infrastructure is for national security (see Figure 28). This recognises that some organisations have a greater role in a country's critical infrastructure and essential national services, such as energy, water, finance, national security and others. Due to this fact, their obligations and compliance with security requirements should be of a higher level than smaller organisations that do not necessarily directly have an impact on critical national services. On the other hand, concerns were raised that prioritising critical infrastructure over non-critical could give a green light to some organisations to be less vigilant. Additionally, vulnerabilities over certain technologies and infrastructure pose an equal threat regardless of the kind of organisation using the technology.

4.5.1.7 Special requirements for CII bodies

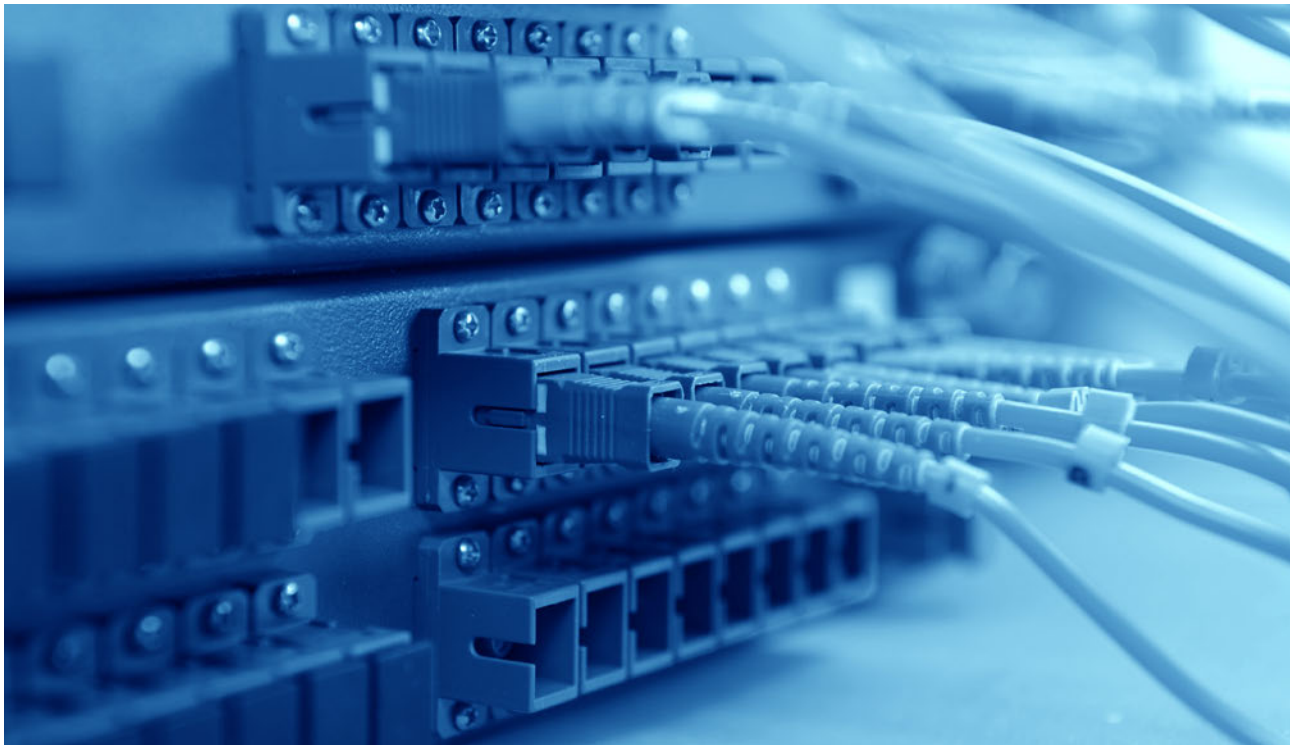
Conclusions

The n/g CERTs have done a lot to foster cross-border cooperation and all have joined (or are in the process of joining) several CERT associations. They use these platforms for exchanging good practices and building trust. Apart from being a member of these initiatives, the n/g CERTs apply the following criteria for determining the credibility of their peers in other countries: technical expertise with a proven track record, ability to respond quickly to security threats and having a stable team. The n/g CERTs commonly engage in bilateral cooperation, which is based not only on the regional aspects, but also on the maturity of the partners. These relationships are not necessarily based on formal agreements. On the domestic front, the n/g CERTs have in most cases formal framework for cooperation with law enforcement authorities; to a lesser degree with other CERTs and ISPs.

Regarding the cooperation capability, a number of deployment shortcomings/gaps have been identified, which are further addressed in the accompanying report 'Baseline Capabilities of national/ governmental CERTS – Updated Recommendations 2012'.

Key identified gaps include:

- Stakeholders at national levels are not sufficiently aware of the existence of n/g CERTs and their responsibilities.
- Constituents among ISPs are unwilling to share information or experience when they are in the presence of their competitors.
- Cooperation with law enforcement authorities can often be one-sided. LEAs are not always in a position to share information.



5

Summary of the Current Status Concerning the Defined Baseline Capabilities

5

Summary of the Current Status Concerning the Defined Baseline Capabilities

N/g CERTs have now been established in the vast majority of the Member States. This represents significant progress compared to the previous document on baseline capabilities, when only about 50% of EU Member States had had an established functional national/governmental CERT. The following key achievements can be reported for the respective category of capabilities:

Mandate and Strategy

- The teams operate on the basis of the mandate from their governments, which can take several forms, from laws and other regulations to more informal forms such as a memorandum. The trend is towards adopting a more formal mandate.
- There is a good level of compliance, with involvement of n/g CERTs in developing of national cyber-security strategies as nearly nine out of ten n/g CERTs claim to be (or have been) involved directly or indirectly in this topic.

Services Portfolio

- The n/g CERTs provide all core services. It is obvious that more mature n/g CERTs are able to provide more extensive services.
- Organising seminars, workshops and providing tutorials has also become a common thing among n/g CERTs.

Operation

- There are provisions across all Member States ensuring that incident handling is (or in the case of newly established n/g CERTs will be) available on a 24/7/365 basis.
- In most Member States the staff numbers more than 8 people, while 6–8 FTEs are considered as necessary for delivering the acceptable level of services on a 24/7/365 basis.

Cooperation

- N/g CERTs in EU Member States actively engage in activities of respective CERT forums such as FIRST, TF-CSIRT, Trusted Introducer or several ENISA initiatives.
- There is a high volume of bilateral and regional cooperation among n/g CERTs, which is driven not only by geographic proximity, but mainly by an immediate need that arises with the emergence of a specific security threat.
- The majority of n/g CERTs operate a working group or another type of umbrella activity that brings together members of the national cyber community for regular meetings to exchange information and expertise.

Despite these achievements there remain areas where action should be taken to further improve the capabilities of the n/g CERTs. These gaps, listed below, are further discussed in the accompanying report 'Baseline Capabilities of national/governmental CERTS – Updated Recommendations 2012':

Mandate and Strategy

- The mandate is not always clear enough, so that it cannot support some activities of the n/g CERTs.
- The mandate is often not made public or sufficiently promoted, which creates doubts on roles and responsibilities of n/g CERTs.
- 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.
- Special provisions including funding needs are missing for the governmental CERT-part functionality.
- N/g CERTs face problems of limited authority when requiring ISPs to handle incidents.
- Data protection legislation is another obstacle for effective incident handling management.

5. Summary of the Current Status Concerning the Defined Baseline Capabilities

Service Portfolio

- When handling incidents internationally, the partnering n/g CERTs do not act in accordance with the information provided, which supports the need for standardised formats in information exchange.
- Vulnerability and artifact handling are not yet fully provided by all n/g CERTs.
- N/g CERTs do not often develop their own tools and services.
- The general statistics on incidents is still not universally made public by n/g CERTs.
- Provision of some of the proactive services like technology watch may be redundant as they are also provided by technology vendors or other CERTs.
- The majority of the n/g CERTs are not involved in disaster recovery planning and business continuity management for CIIP.

Operation

- The n/g CERTs rely on state funding and are not active enough in looking for additional resources.
- Legal and PR experts are missing from the staffs of n/g CERTs.
- The teams also face difficulty in recruiting highly specialised personnel, for example in areas of reverse engineering or digital forensics.
- There are not many opportunities in Europe for training in deep technical aspects.
- Although the teams mostly provide their core services on a 24/7 basis, this functionality is not often displayed on the n/g CERT's websites.
- Constituents are satisfied with templates provided for reporting incidents but call for data exchange to be more automated.

Cooperation

- Stakeholders at national levels are not sufficiently aware of the existence of n/g CERTs and their responsibilities.
- Constituents among ISPs are unwilling to share information or experience when they are in the presence of their competitors.
- Cooperation with law enforcement authorities is one-sided, as LEAs are not in a position to share much information.

This report may serve as guidance on the current status of deployment of baseline capabilities, while identifying shortcomings on the part of n/g CERTs as well as other stakeholders. These gaps are handled specifically by the accompanying report 'Baseline Capabilities of national/governmental CERTs – Updated Recommendations 2012'. They are also possible topics for ongoing cooperation among n/g CERTs and for workshops and initiatives of ENISA aimed at collecting best practices and thus further facilitating the operation of n/g CERTs in the Member States.

6

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

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, like academia, companies, governments or the 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 to become more universal providers of security services.

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.

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.

Annex I: Glossary

National / governmental 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' is introduced. Still vague, this term depicts the following kind of CERT:

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

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.

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.

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.

Annex II: Abbreviations

ACID	Analysis Console for Intrusion Databases
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
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
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
HTTPS	Hypertext Transfer Protocol Secure
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
KPIs	Key Performance Indicators
LEA	Law Enforcement Authority
MoU	Memorandum of Understanding
NATO	North Atlantic Treaty Organization

Annex II: Abbreviations

NCSS	National Cyber-security Strategies
NIST	National Institute of Standards and Technology
NRA	National Regulatory Authority
OECD	Organisation for Economic Co-operation and Development
OTRS	Open Ticket Request System
PGP	Pretty Good Privacy
PoC	Point of Contact
PPP	Public Private Partnership
PTE	Part-Time Employee
RFC	Request for Comments
RSS	Rich Site Summary
RTIR	Request Tracker for Incident Response
S/MIME	Secure/Multipurpose Internet Mail Extensions
SANS	SysAdmin, Audit, Networking, Security
SSH	Secure Shell
SSL	Secure Sockets Layer
TERENA	Trans-European Research and Education Networking Association
TETRA	Terrestrial Trunked Radio
TI	Trusted Introducer
TLD	Top Level Domain
TLP	Traffic Light Protocol
WP	Work Programmes

Annex III: Web resources

- Websites of national/governmental CERTs and other CERTs in the Member 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, number of websites in all 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 indicate 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?

Annex IV: Questionnaire for national/governmental CERTs

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 hosting organisation, or are there just arrangements within the hosting organisation (internal agreement or policy)?

A8. Is your hosting 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 hosting 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.

Annex IV: Questionnaire for national/governmental CERTs

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 hosting 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 agencies? Please identify the type of law enforcement agencies 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 organization (please indicate in the table below)?:

Type of Your Organisation	Insert an 'x' Next to the Relevant Type
CERT	
Policy maker (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)	

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

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):

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 organization'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?

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

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.)?

Annex VI: Discussion Guide for Interviews

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: n/g CERT maturity model and services

N/g CERT Maturity Model

National/governmental CERT capability maturity model

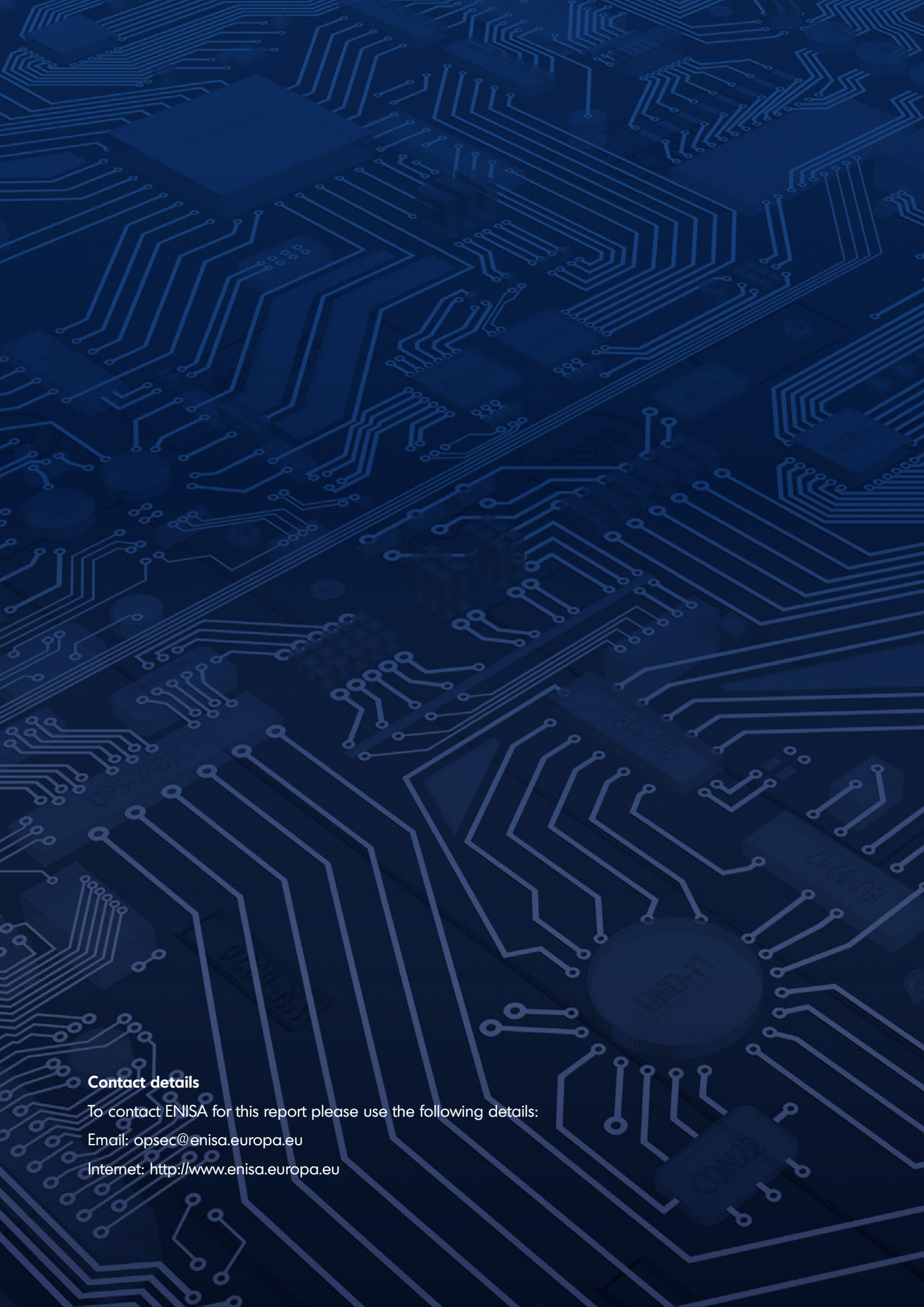
Optimised	• The CERT has full official mandate for all national/governmental CERT responsibilities • The CERT has longstanding, excellent trust relationships with its constituency, stakeholders and peers • CERT services are mature and focus is on continually improving process performance through both incremental and innovative technological changes/improvements
Managed	• The CERT has official mandate in certain national/governmental CERT responsibilities and has full recognition in the CERT community (including FIRST membership and Trusted Introducer certification) • Using process metrics, management can effectively control the core CERT processes. Other CERT services offered, are defined and documented processes, providing consistent and quality results
Defined	• The CERT has official mandate in certain national/governmental CERT responsibilities and has full recognition in the CERT community (including FIRST membership and Trusted Introducer certification) • Using process metrics, management can effectively control the core CERT processes. Other CERT services offered, are defined and documented processes, providing consistent and quality results
Repeatable	• Regular contact with other national/governmental CERTs, trust relationships are cultivated • All core CERT services are provided. Some non-core (added value) CERT services may be initiated • Core CERT service processes are repeatable, with consistent results. Certain processes supporting the CERT services are documented
Initial	• Contact with other national/governmental CERTs and recognition in the CERT community is limited • Certain core CERT services are provided • Processes supporting the CERT services are undocumented, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events

Source: ENISA – Baseline Capabilities for national/governmental CERTs: policy recommendations

CERT Service Portfolio Table

Reactive Services	Proactive Services	Artifact Handling
Alerts and Warnings Incident Handling Incident analysis Incident response support Incident response coordination Incident response on site Vulnerability Handling Vulnerability analysis Vulnerability response Vulnerability response coordination	Announcements Technology Watch Security Audits or Assessments Configuration and Maintenance of Security Development of Security Tools Intrusion Detection Services Security-Related Information Dissemination	Artifact analysis Artifact response Artifact response coordination **Security Quality Management** Risk Analysis Business Continuity and Disaster Recovery Security Consulting Awareness Building Education/Training Product Evaluation or Certification

Source: http://www.enisa.europa.eu/activities/cert/support/guide/strategy/services



Contact details

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

Email: opsec@enisa.europa.eu

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

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

Contact details

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

Email: opsec@enisa.europa.eu

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