Version 1.0 (initial draft)

Baseline Capabilities of National / Governmental CERTs
Part 2: Policy Recommendations

enisa
European Network and Information Security Agency

Table of Contents

EXECUTIVE SUMMARY

1 – Executive Summary

This document constitutes a very first attempt to define a minimum set of capabilities that a Computer Emergency Response Team (CERT) in charge of protecting critical information infrastructures in Member States should possess in order to take part in and contribute to sustainable cross-border information sharing and cooperation. It is aimed mainly at supporting policy- and decision-makers in the EU Member States in the establishment of a suitable framework that will enable their national / governmental CERTs to operate properly, by shedding a light on policy requirements and experiences in the Member States and also by providing some background information on the operations of CERTs so that their requirements and needs are understood better.

It is therefore also advisable that decision-makers in national / governmental CERTs (or project leaders and members of the teams, as appropriate) take note of this document so that they will be prepared for a dialogue with policy-making bodies, which this document cannot replace.

Member States should establish by 2012 a well-functioning network of CERTs at national level covering all of Europe.

European Commission - A Digital Agenda for Europe - COM (2010) 245

The recommendations presented in this document focus on the appropriate implementation of national / governmental CERTs to strengthen the security and resilience of national (critical) information infrastructures. These recommendations are in line with the communications of the European Council and the Commission which address the challenges and priorities for network and information security (NIS) and critical information infrastructure protection (CIIP), and the establishment of the most appropriate instruments needed to tackle those challenges at the level of European Member States. However the recommendations do not constitute a one-size-fits-all guide. Member States will need to scrutinize the recommendations and, with the help of ENISA, decide if they are appropriate in the context of their present national situation.

More specifically, policy recommendations have been formulated, in line with a previous ENISA publication Baseline capabilities for national / governmental CERTs [10], in the following areas:

Mandate and strategy

National / governmental CERTs need a clear mandate to serve a well-defined constituency which is supported on a sound legal basis. Their role should be embedded in the strategy for national cyber-security and established in an appropriate body with adequate funding.

Service portfolio

Several types of services can be offered by a national / governmental CERT, and these should be clearly defined in line with its mandate and strategy. It is recommended that they include proactive and reactive services as well as additional management services for security quality. Appropriate internal processes should also be implemented to support the external services.

Operation

It is recommended that the operation of a national / governmental CERT be subject to appropriate practices of good governance. More specifically, consideration should be given to the appropriate management of certain aspects of internal organisation, the supporting infrastructure, service delivery and business continuity.

Cooperation

The effectiveness of national / governmental CERTs is highly dependent on cooperation with various other cyber-security stakeholders, on the national and trans-national levels. It is therefore strongly recommended that these relationships be facilitated and fostered by building trust, ensuring the quality of information, using common terminology, etc.

Disclaimer

The document in its current status is in no way to be considered final, but rather as the record of an ongoing process. This process was begun by ENISA in 2009 with an all-embracing survey among all (120+) known CERT teams in Europe and was, together with the EU Member States and their national / governmental CERTs and with the help of Deloitte as an external consultant, continued in 2010.

This document is therefore to be considered a work-in–progress that will undergo necessary changes in the future in accordance with an ongoing dialogue with all relevant stakeholders, which is reflecting the ongoing changes taking place in the European NIS landscape.

In some areas of the capabilities of national / governmental CERTs the proposed requirements are quite stable, while in other areas additional research, analysis and comprehensive discussions with the stakeholders involved are necessary. Having a national / governmental CERT in place that fulfils the requirements for 'baseline capabilities' as defined in this document is essential for CIIP in all Member States. However these teams should not be considered as the one and only necessary measure a Member State must take in order to ensure adequate protection. CIIP at the national level must always be planned as part of a complete cyber-security strategy, in which a national / governmental CERT plays an important role but is not the only component. The planning of a complete national cyber-security strategy in a Member State is outside the scope of this document; however this document does provide an insight into the role these teams can play and how they could be embedded in such strategy.

INTRODUCTION

2 – Introduction

2.1 – Target audience

The primary target audience for the recommendations in this document are those policy-making bodies in the European Union Member States that are responsible for initiating and planning the establishment and operation of a national / governmental CERT and are responsible for creating an adequate national policy framework for these tasks.

2.2 – Report objective

The key objectives of this document are:

- to guide policy- and decision-makers at the national level in creating appropriate policy for building the capabilities of national and governmental CERTs;
- to help bridge possible discrepancies between the views of technical experts and decision-makers in setting and implementing correct policies for the capabilities of national and governmental CERTs.

2.3 – Context

The risks related to cyber-attacks are ever-growing, and threats from unknown sources are dynamic and constantly evolving. More frequently than ever before, reports on significant security incidents are being given prominence in the media, illustrating an increasing need for the effective and efficient management of cyber- security. Computer Emergency Response Teams (CERTs[1]) are playing an increasingly important role in this regard as they are responsible for collecting information about and coordinating the response to cyber-security incidents.

ICT systems and networks form a vital part of the economy and society of the Europe Union and its Member States. For this reason, they are generally regarded as critical information infrastructure (CII), as their disruption or destruction would have a serious impact on vital societal functions. More specifically, CIIs are those systems that provide the resources upon which all the functions of society depend, such as telecommunications, transportation, energy, water supplies, healthcare, emergency services, manufacturing and financial services, as well as essential governmental functions. As a consequence, every single country that is connected to the internet has an interest in the implementation of capabilities to effectively and efficiently respond to cyber-security incidents, and protect these essential functions from a national security perspective.

Initially, CERTs were mainly established to provide security incident management services for particular private sector or academic constituencies. However, an emerging need for national / governmental CERTs to support incident management across a broad spectrum of sectors within a nation's borders has presented itself. Moreover, national / governmental CERTs have become key components in the implementation of cyber-security and critical information infrastructure protection (CIIP) at the national level.

Objective of a national / governmental CERT

The main goal of a national / governmental CERT, from a cyber-security perspective, is to protect national and economic security, the ongoing operations of a government, and the ability of critical infrastructures to continue to function. Therefore a national / governmental CERT typically monitors incidents at a national level, identifies incidents that could affect critical infrastructures, warns critical stakeholders about computer security threats, and helps to build organizational CERTs in the public and private sectors.

1 It should be noted that, in general, the terms CERT and CSIRT (Computer Security Incident Response Team) are often interchanged, though the first is actually a registered trademark of Carnegie Mellon University.

2.4 – Policy environment

At the global policy level, the United Nations General Assembly adopted a resolution in 2004 on the Creation of a global culture of cyber-security and the protection of critical information infrastructures **[36]**. This resolution recognizes the importance of cyber-security and provides various high level strategic recommendations for UN Member States.

Given the importance of protecting the critical infrastructure of our online society in these times and the fact that the European Commission placed this consideration high on the European Digital Agenda in May 2010, it is essential for Member States to undertake further action. On December 8th 2008 the Council adopted a Directive on Critical Infrastructure Protection **[21]**, the purpose of which was to identify and designate European critical infrastructures (ECI) that would benefit from a common approach to the improvement of their protection.

Additionally, in a resolution of December 18th 2009 **[20]**, the European Council recognised the need for a collaborative European approach to network and information security. This resolution calls upon Member States, the European Commission, ENISA and other stakeholders to increase efforts to enhance the level of network and information security and to improve collaboration in order to achieve this.

Furthermore, the proceedings of the 2009 Tallinn EU ministerial conference on CIIP **[18]** suggested an action plan that provides a sound basis for increasing the effectiveness of the fight against cyber-crime and cyber-terrorism. This plan is aimed at improving preparedness as a first line of defence, but also highlights the importance of taking due consideration of both the economic and societal dimensions of enhancing resilience and stakeholder responsibility. It states that each EU Member State should act domestically to enhance the protection of its own critical information infrastructures as a necessary building block for enhanced preparedness in the EU. In this context, the establishment of well-functioning national / governmental Computer Emergency Response Teams (CERTs) and incident response operations should be accomplished as a step towards effective pan-European cooperation.

In the 2009 Communication of the European Commission on Critical Information Infrastructure Protection **[16]**, a number of key challenges are highlighted and a concrete action plan is presented as a response to these challenges. This action plan also includes a number of elements regarding national / governmental CERTs where the Commission invites Member States and concerned stakeholders to:

- define a minimum level of capabilities and services for national / governmental CERTs and incident-response operations in support of pan-European cooperation;
- make sure national / governmental CERTs act as key components of their national capability for preparedness, information sharing, coordination and response;
- strengthen the cooperation between national / governmental CERTs by, eg, leveraging and expanding existing mechanisms for cooperation such as the European Government CERTs (EGC[2]) group.

Deadline for the implementation of national / governmental CERTs

In its 2009 communication on CIIP [16], the European Commission specified the target deadline for establishing well-functioning national / governmental CERTs in all Member States as the end of 2011. The active role of ENISA is called upon to stimulate and support the pan-European cooperation between national / governmental CERTs that would lead to enhanced preparedness, a reinforced European capacity to react and respond to incidents, and pan-European (and/or regional) exercises.

2 http://www.egc-group.org

The European Commission is also defining a strategy for European cyber-security and the protection of critical information infrastructure. It has published various communications and directives on this subject and has also incorporated cyber-security and CIIP in new communication Digital Agenda for Europe [14].

2.5 – Glossary

In this section, certain key terms regarding national and governmental CERTs are clarified.

CERT/CSIRT: A computer emergency response team (CERT) is a service organisation responsible to a defined constituency for responding to cyber-security incidents. It provides the necessary services for handling incidents and supports its constituents in their recovery from breaches of computer security. In order to mitigate risks and minimise the number of required responses, most CERTs also provide preventative and educational services for their constituencies. The constituency (an established term for the customer base) of a CERT usually belongs to a specific sector, such as academia, companies, governments or military. The term CSIRT (computer security incident response team) is a more modern synonym which illustrates the fact that CERTs developed over time from merely reactive forces into more universal providers of security services.

National CERT: A national CERT acts as a national point of contact (PoC) for collaboration and information sharing (such as incident reports and information on vulnerabilities) with other national CERTs in EU Member States and worldwide. National CERTs can also be considered as the CERT-of-last-resort for the national domain, which is a unique national point of contact with a coordinating role. In many cases a national CERT also acts as the governmental CERT. It should be noted that definitions may vary across Member States.

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

Governmental CERT: A governmental CERT is responsible for the protection of governmental and public administration networks. The constituency of a governmental CERT therefore is the government and other public bodies. It should be noted that, in many cases, military CERTs are considered separately due to their particular remit. Current practices illustrate that in many cases governmental CERTs also act as national CERTs. It should be noted that definitions may vary across Member States.

In the context of this document and ENISA's work in the area of baseline capabilities, the term **national / governmental CERT** has been introduced to cover the terms 'national CERT' and 'governmental CERT' as described above. The term 'national / governmental CERT' therefore subsumes all the 'flavours' of national CERTs, governmental CERTs, national points of contacts, etc, in the EU Member States which are:

- 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 their countries;
- acting as official national points of contact for national / governmental CERTs in other Member States.

2.6 – Current state of national and governmental CERTs

Various national cyber-security initiatives have been or are being implemented to strategically address incidents related to key resources and critical infrastructures, as well as to build a community of CERTs. The most typical goals of these initiatives include:

- establishing a national focal point within a country or region to coordinate security incident management activities;
- analyzing and synthesizing information on incidents and vulnerabilities disseminated by other CERTs, vendors and technology experts to provide an assessment for their own constituencies and communities;
- facilitating communications across a diverse constituency, in order to bring together multiple sectors (government and military, critical services and infrastructures, commercial, academic, banking and finance, transportation, etc) to share information and collaborate in addressing computer security problems, such as widespread computer security incidents, threats and vulnerabilities;
- developing protocols and mechanisms for trusted interaction with other relevant stakeholders such as the intelligence community, law enforcement agencies, policymakers, etc.

Most European countries have in fact already moved forward in establishing and operating national / governmental CERTs. These teams are expected to act as primary providers of security services for society and their governments, despite the fact that, in certain cases, they have not been officially mandated or are not supported by public resources.

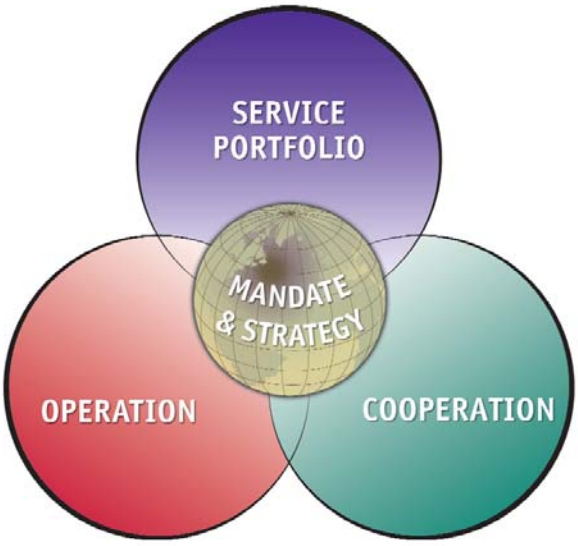
Over the years, many national and governmental CERTs in EU Member States have been extending their capacities from being merely reactive forces to providing more comprehensive cyber-security services, including proactive services such as alerts, security advisories, security management services, etc. These CERTs have become, or are still increasingly becoming, key components for the implementation of critical information infrastructure protection (CIIP) at a national level.

Although there are commonalities regarding the challenges of cyber-security risks and policy developments, the actual state and maturity of national / governmental CERTs differs across Member States. It should be noted that a purely national approach runs the risk of fragmentation and the creation of inefficiencies across Europe as there are differences between national approaches. Furthermore, a lack of systematic cross-border cooperation negatively affects the effectiveness of all efforts due to increasing cross-border dependencies.

2.7 – Document outline

In 2009, to guide policy- and decision-makers in the Member States in the creation of appropriate policies for building the capabilities of national / governmental CERT, ENISA, together with well known CERTs in Europe, developed a series of key baseline recommendations in four areas:

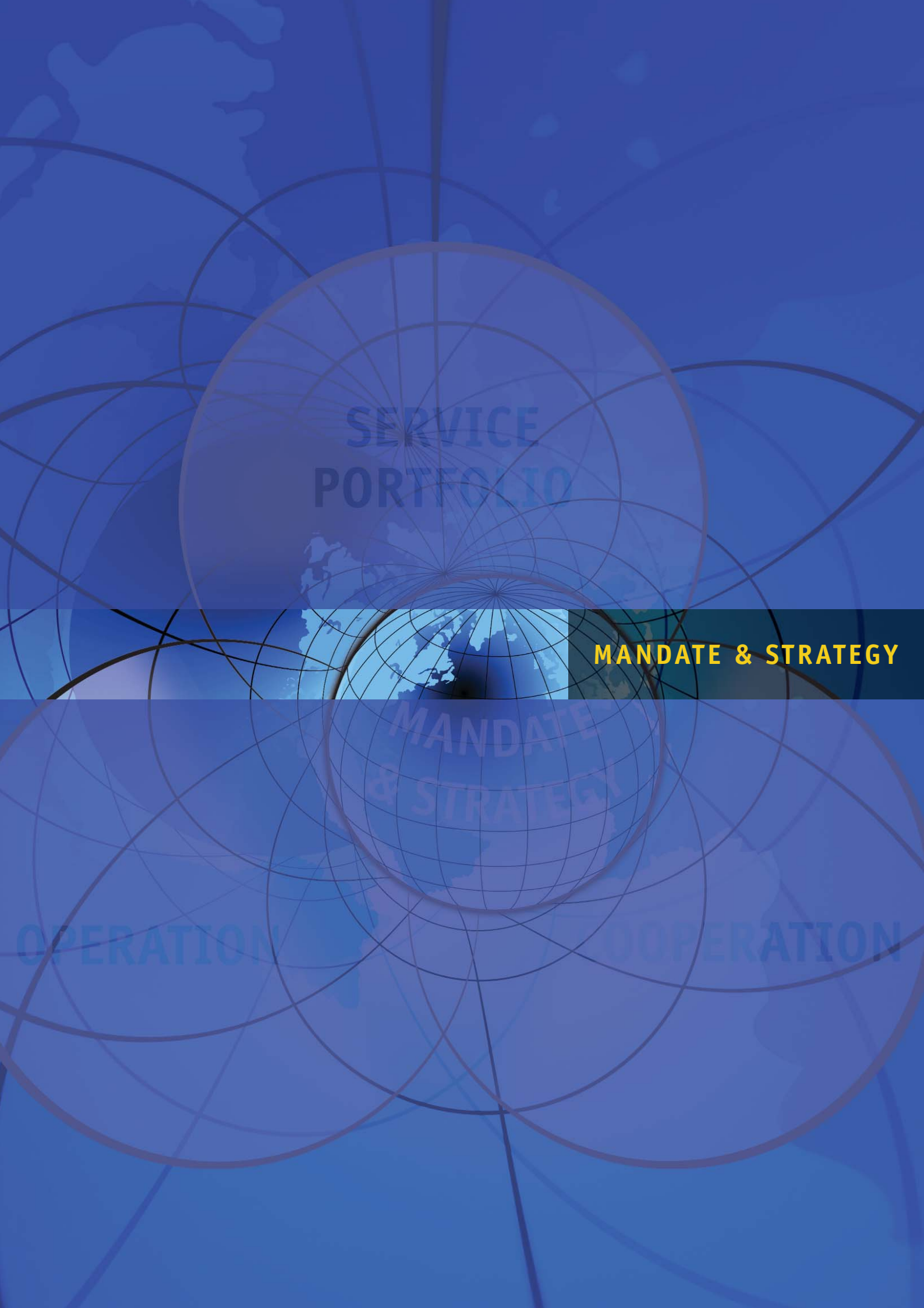
- mandate and strategy
- service portfolio
- operation
- cooperation.



These have been aligned with the previous ENISA publication Baseline capabilities for national / governmental CERTs [10].

A series of key considerations and policy recommendations for each of these areas are elaborated further in the chapters that follow in this document.

To conclude this document, a roadmap for the implementation of a high-level national / governmental CERT and an initial proposal for a maturity model for the capabilities of national / governmental CERTs are included in Annex B. The implementation roadmap is intended to help policy- and decision-makers at the different phases of implementation of a national / governmental CERT. The capability maturity model provides an initial indicative overview of the maturity levels of national / governmental CERTs.



MANDATE & STRATEGY

3 – Mandate & Strategy

3.1 – National cyber-security & CIIP strategy

Today, policymakers have a better understanding of the importance of and challenges in protecting not only government information but also the critical infrastructures that support their economies and the broader public interest within their borders. They are seeking effective and coordinated approaches in their responses to cyber-incidents, threats and attacks that can affect both the public and private sectors. One of the highlights of the European Commission's public consultation document Towards a strengthened network and information security policy in Europe [19] is the need for a holistic approach to cyber-security and the protection of critical information infrastructures.

In order to develop an appropriate cyber-security strategy, a number of key actions need to be performed:

- establishment and development of cyber-security as part of national policy;
- identification of a leader in the overall national effort as well as appropriate experts and policymakers within the public and private sectors, and the establishment of cooperative arrangements among stakeholders;
- identification of expert counterparts internationally and the fostering of initiatives in collaboration;
- establishment of an integrated risk management process for identifying and prioritizing protective measures regarding cyber-security;
- assessment and periodic reassessment of the current state of cyber-security efforts and the development of programme priorities.

A strategy on CIIP and cyber-security is being or has already been implemented in several countries but, overall, there are still many opportunities for development in this area. As indicated in the description of the policy environment in section 2.4 above, both at the European and the global levels, a strong capability to respond to incidents is identified as a key component of an overall strategy for cyber-security and CIIP.

A complete national CIIP capability should typically include the establishment of a mandated (governmental) actor for strategic leadership and governance, a coordination centre, and a centre for technical expertise (CERT), all of which would interact with specific stakeholders at their level. This implies that a state should set up a coordinated national system capable of responding to cyberspace security threats, which should include a national / governmental CERT to prevent, detect, deter, respond to, and recover from cyber-incidents.

The maturity of national cyber-security and CIIP strategies and the roles of national / governmental CERTs in these strategies are currently not harmonized between countries and depend strongly on the specific context of a country. What is indisputable, however, is that national / governmental CERTs have a key role to play within any cyber-security or CIIP strategy from multiple perspectives, such as information sharing and the coordination of responses to incidents, reporting, etc.

A multi-stakeholder, multi-level approach is essential, taking place at the European level while fully respecting and complementing national responsibilities.

Communication of the European Commission on Critical Information Infrastructure Protection - COM(2009)149

Recommendations:

- *Member States should consider adopting a holistic, coordinated national approach to cyber-security and CIIP that is aligned with the European strategy, its policy context and risk management practices. Member States should make sure that all relevant stakeholders are involved in the national approach to these issues and their roles are clearly identified, including the role of the national / governmental CERT.*

- *National / governmental CERTs should be key components of national cyber-security and critical information infrastructure protection strategy. Consequently, the roles of the national / governmental CERTs should be translated into formal mandates with detailed specifications of the capabilities required to carry out these mandates.*

3.2 – Mandate

In the context of a national strategy for cyber-security, a national / governmental CERT should play a key role, next to other key players and stakeholders such as, for instance, national regulatory authorities, industry associations (eg, telecoms, banking and energy), and justice and law enforcement departments. On the basis of that strategy, a national / governmental CERT should be mandated and given a specific set of roles and responsibilities and an official framework within which it is to work.

Host organisation

The official, legal framework within which the national / governmental CERT must work sometimes depends on the host organisation in which the CERT is located. In other cases, the official, legal framework should be defined by the official mandate given by the government.

A common situation is that the host organisation of the national / governmental CERT is a national telecommunications regulatory authority (NRA). When the CERT is embedded within an NRA, it is then possible to make use of the official framework of the NRA, taking advantage of, for example, its authority over telecommunications providers in crisis situations.

However, more recently, a popular development (within Europe as well as internationally) is the creation of a 'national cyber-security centre', which is responsible for the national cyber-security strategy. Such an organisation would, for example, include a coordinating office responsible for strategic leadership and the coherence of the national strategy (in the public and private sectors), and a national / governmental CERT. Examples of nations that have recently implemented such an organisational structure are the United Kingdom [34] (see the conclusions of the report *Cyber Security Strategy of the United Kingdom* in the textbox below), France, the United States of America, and Japan.

Illustration of a national cyber security strategy implementation:

Cyber Security Strategy of the United Kingdom – Conclusions

To address the UK's cyber-security challenges, the Government will:

- ***Establish a cross-government programme;***
- ***Work closely with the wider public sector, industry, civil liberties groups, the public and with international partners;***
- ***Set up an Office of Cyber Security (OCS) to provide strategic leadership for and coherence across Government;***
- ***Create a Cyber Security Operations Centre (CSOC).***

Depending on the host organisation, the national / governmental CERT will report to different levels in the government. Where it is embedded in a host organisation that does not deal directly with cyber-security, the reporting chain will need to pass through the host organisation in order to reach the national executive. In cases when the CERT is part of a national cyber-security centre, that organisation often falls directly under the power of the national executive.

Recommendations:

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

Constituency

The constituency of a CERT is an established term for the customer base for its services. So, in theory, the constituency of a national / governmental CERT consists of all entities with the state's borders. This is due to the fact that any domestic entity is a potential customer of the national / governmental CERT. The constituency of a national / governmental CERT can typically be broken down into subgroups, according to the services the CERT delivers to the entities in the group or based on the responsibilities the CERT carries with regards to the group. Typically, the following constituency subgroups can be distinguished:

- Government and public bodies:
  The national / governmental CERT will provide its full range of services to the government and public bodies.
- Critical information infrastructure organisations: The national / governmental CERT may provide its full range of services to CII organisations. In most cases, however, CII organisations in private hands will have IT or information security personnel responsible for handling security incidents. In such cases, the national / governmental CERT may play a more coordinating or supporting role.
- Other stakeholders within the state's borders: As the CERT-of-last-resort and national point of contact for cyber-security incidents, the national / governmental CERT will provide a subset of its services to any other domestic stakeholders or the broad public interest.

Depending on how the national / governmental CERT has come into existence, other groups of constituents may be distinguished as well. For example, research and education networks will remain a special group of constituents for a research/education network CERT that has become the de facto national / governmental CERT.

In any case, when the national / governmental CERT receives an incident report from a domestic or foreign source, it will verify whether the affected entity belongs to a CERT's constituency. If the affected entity belongs to another CERT's constituency, the national / governmental CERT will, like any other CERT, forward the incident report to the appropriate body. If the concerned entity is a government or public body, or is a critical information infrastructure organisation, or is not part of another CERT's constituency, the national / governmental CERT will handle the incident report. Obviously other CERTs (domestic, non-national / governmental CERTs or foreign CERTs) will perform the same evaluations of incident reports and forward the reports to the appropriate CERT.

Recommendations:

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

For resource-related reasons, the full scope of services should only be provided to privileged constituents such as the government, public bodies and critical information infrastructure organisations. Non-privileged constituents receive by default only a subset of the full range of services. However, on a case-by-case basis, the national / governmental CERT could also provide additional services to non-privileged constituents.

Roles and responsibilities for the national / governmental CERT

The generic roles and responsibilities of a national / governmental CERT are inherently linked to the services it delivers to its constituency, which are discussed in chapter 4 – Service Portfolio. In general terms, a national / governmental CERT [10] has a number of specific roles in its country, including:

- generally supporting the management of security incidents for systems and networks within its state's borders;
- bearing responsibilities for contributing to the protection of critical information infrastructure (CIIP) within the state as part of wider CIIP arrangements;
- acting as the official national point of contact for national / governmental CERTs in other Member States and world-wide.

An official mandate from its government to represent the country in international CERT communities, such as FIRST[3] (Forum of Incident Response and Security Teams) and potentially EGC (European Government CERTs), is crucial for a national / governmental CERT. This mandate must include provisions for the team to act as the official national point of contact (PoC) for CERTs (and other members of the security community) in other countries as this is an indispensable element of the national CIIP plan and is required for clear and flexible international collaboration.

The role of official national PoC for CERTs naturally brings with it the responsibility to act as a CERT-of–last-resort that is available, in situations of doubt and emergency, to relay incident reports (and other security related information) to the appropriate entities in its country (eg, by forwarding the incident report to the IT or information security departments of affected companies). If no other appropriate entity can be found to deal with a cyber-security incident, the national / governmental should consider handling the incident.

As stated in the previous section, a national / governmental CERT should be part of holistic national cyber-security and CIIP strategies. National goals regarding the protection of critical information infrastructures cannot be reached however without strong public-private partnerships, as most infrastructures are privately owned. Within the CIIP strategy, the national / governmental CERT can therefore play various roles. Depending on the roles of other organisations, the national / governmental CERT should bear responsibilities or play an active or passive role throughout the whole process of defining the scope of CIIP, identification of CII, assessment of the 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.

In some cases, the national / governmental CERT is involved in the full process and bears responsibilities with regards to the implementation and monitoring of the national CIIP plan. In fact, the national / governmental CERT should be part of the CIIP plan, as significant security incidents in relation to CII will need to be reported to the national / governmental CERT and the CERT will have a coordinating role in crisis situations.

These specific functions are elaborated in the following chapters. Aside from the three previously mentioned functions, a national / governmental CERT may also take on other roles and responsibilities. These could include, for example, helping public and private institutions and organisations within the country by providing wider expertise with regards to cyber-security. Another role could consist of organizing, participating in, and promoting sectoral or topic-specific initiatives in collaboration.

3 http://www.first.org/

Recommendations:

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

SERVICE PORTFOLIO

4 – Service Portfolio

The service portfolio of any national / governmental CERT will consist of the external services it provides to its constituency and its internal support processes.

External CERT services are commonly categorized into three service classes:

- Proactive services, aimed at improving 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 reduce their impact and scope when they do occur.
- Reactive services, aimed at responding to requests for assistance, reports of incidents from the CERT constituency, and tackling threats or attacks against the CERT's systems.
- Other security quality management services, which are the common services designed to improve the overall security of an organisation. By leveraging the unique experiences gained in providing reactive and proactive services to its high-value constituency, a national / governmental CERT finds itself in a special position to apply those experiences to these quality management services. These services are designed to incorporate feedback and lessons learned based on knowledge gained in responding to incidents, vulnerabilities and attacks.

It should be noted that these services require appropriate internal support processes such as, for example, resource or infrastructure management processes. These supporting processes should also receive adequate consideration as they are the keys to the continuous improvement of the maturity of a national / governmental CERT.

National / governmental CERT core capabilities

A number of core capabilities concerning the service portfolio are generally considered as the most critical to the operation of a typical national / governmental CERT.

- **Incident handling**
  The only certainty within cyber-security is the fact that 100% security does not exist. Security incidents will happen, no matter what. Without an effective incident handling capability, attacks and intrusions on critical national information infrastructure could cripple the state for the duration of the attack. Consequently, handling cyber-security incidents on a national (and cross-border) scale, and incidents related to critical information infrastructure, are a priority for a national / governmental CERT. Incidents related to critical information infrastructure can pose a direct threat to society (economic, governmental, infrastructural or ecologic threats) and the lives of a state's citizens (eg, in the case of an incident at a nuclear power plant). These incidents should therefore receive priority over all ongoing activities and be contained and mitigated as quickly as possible.
- **National point of contact for incident reporting and information dissemination**
  Probably the second most important task performed by a national / governmental CERT is its role as the national point of contact for reports on incidents and the dissemination of security-related information. This is one of the responsibilities that must be officially mandated by a government to its national / governmental CERT in order to achieve clear and flexible national and international collaboration. Foreign CERT teams must clearly know whom to contact with regards to the sharing of security-related information and the reporting of incidents. Additionally, the national / governmental CERT is best positioned to further disseminate such information (alerts, warnings, announcements, vulnerabilities, etc) among the other CERTs in the country and the information security communities. In addition, the national / governmental CERT will also represent the country in international CERT communities by virtue of this official mandate.

- **Critical information infrastructure protection**
  The role of a national / governmental CERT in national CIIP is not fixed. Several services could be provided in addition to the incident handling service. Examples include risk analysis, security consulting, security assessment, intrusion detection services and many other services. The exact role of the national / governmental CERT will depend heavily on the national strategy for CIIP.

In the context of CIIP, besides the services listed above, it is advisable for national / governmental CERTs to provide additional services such as:

- announcements informing constituents about new developments with medium- to long-term impact, such as newly found vulnerabilities;
- security-related information sharing that provides constituents with a comprehensive and easy-to-find collection of useful information and guidelines for improving security;
- alerts and warnings involving the dissemination of information that describes an intruder attack, security vulnerability, intrusion alert, computer virus or hoax, etc, and providing a short-term recommended course of action for dealing with the resulting problem;
- awareness building that provides information and guidance for conforming better to accepted security practices and organisational security policies.

These services deliver tangible added-value to the constituency in an efficient manner, as the information needed to provide these core services can be leveraged for the entire constituency. Additionally, security notifications and other information for the constituents also greatly improve the visibility and the standing of a national / governmental CERT and facilitate the building of trust in the capabilities of a team.

Most national / governmental CERTs subdivide their constituencies and offer 'free' services (such as announcements and alerts, which are not highly dependent on the target audience) to the public, but deliver additional resource-intensive services (incident response, vulnerability handling, artifact analysis, etc) only to the government, public institutions and critical information infrastructure entities. As a CERT-of-last-resort, it usually cannot provide the same level of service to the public, due to high demand for its resources and staffing.

A strong European early warning and incident response capability has to rely on well functioning national / governmental CERTs.

Communication of the European Commission on Critical Information Infrastructure Protection - COM(2009)149

The service portfolio of a national / governmental CERT will mainly depend on its mandate and on resource and staff constraints. When resources are scarce, it is better to start with just the core services.

Depending on the mandate given to the national / governmental CERT and on how national bodies related to cyber-security have been established within the government structure, certain added-value, non-core services of the traditional CERT service portfolio may also be provided by a national standards organisation, a national cyber-security coordination centre, or security operations centre or some other body. These could include, for example, product evaluation or certification, awareness building, the development of security tools, monitoring, etc.

The following sections elaborate further on these matters and provide recommendations concerning the services of national / governmental CERTs under the categories introduced above.

4.1 – Proactive services

The main objective of proactive services is to help in reducing the number of cyber-security incidents through the implementation of preventive measures that secure the systems, processes and people of the national / governmental CERT and its constituents.

Although most CERTs only provided responsive services when they were first established, currently they are very much focused on proactive services. The final objective of security-incident management is to minimize the impact of a cyber-security incident. The best way to achieve this goal is to prevent the incident from happening in the first place. The following are examples of proactive services a national / governmental CERT could offer.

- Technology watch, announcements, and the dissemination and sharing of security-related information could provide early warnings of threats or vulnerabilities and help the constituency protect its systems before it is too late.
- Security assessments could aid the constituency in mitigating existing vulnerabilities in their infrastructure.
- Providing guidelines on security configuration could assist the constituency in hardening their systems in order to minimize the attack surface and reduce the residual risk.
- Providing intrusion detection services could help the constituency to detect ongoing attacks or intrusions, and to initiate the incident handling process as soon as possible.

Illustration: EISAS (European Information Sharing and Alert System)[1]

There are many systems and initiatives across Europe that have the goal of disseminating appropriate and timely information on network and information security (NIS) vulnerabilities, threats, risks and alerts, as well as sharing good practices. In 2006, ENISA was asked to analyse the current state of affairs as regards such systems and initiatives in the public and the private sectors in the EU Member States and to identify possible sources of security information that could potentially contribute to a Europe-wide information-sharing and alert system (EISAS).

Two types of involvement for the European Union (operating and facilitating) in the three parts of the information sharing process (information gathering, processing and dissemination) were examined under three different perspectives (technical & organizational, political and socio-cultural). The study concluded that the most effective level of involvement for the European Union in the establishment and operation of an information sharing system for its home-users and SMEs would be that of a facilitator, moderator of discussions and a 'keeper of good practice'. The report closed with proposals for the next steps to be taken and a 'proof of concept' scenario.

[1] http://www.enisa.europa.eu/act/cert/other-work/eisas

4.2 – Reactive services

As previously remarked, an IT system that is perfectly secure does not exist. It is only a matter of time before a vulnerability is found and exploited. In order to prepare for such cyber-security incidents, a comprehensive framework needs to be setup to ensure a timely and effective response. A national / governmental CERT is responsible for coordinating responses to incidents reported by its constituency.

To prevent an incident from escalating to a crisis or disaster, a timely and effective response is needed and, due to the fact that most critical information infrastructure is operated by private companies, a coordinated response by the government and private sectors to attacks on government and critical information infrastructures is required.

This comprehensive framework for responses to cyber-security incidents should empower the national / governmental CERT to undertake the following tasks:

- Incident handling: the incident response capabilities with regards to critical information infrastructure will mainly rely on the implementation of adequate institutional structures to support these responses.
- Issuing alerts and warnings: alerts and warnings can be based on inter-CERT communications, incidents that happened in the constituency and/or detected vulnerabilities.
- Vulnerability handling: in order to provide high-quality vulnerability alerts, counter-measures and expert incident handling, the national / governmental CERT needs to receive information about and to be able to analyse system vulnerabilities.
- Artifact handling: to be able to provide high-quality alerts on new malware and other artifacts and to provide expert incident handling, the national / governmental CERT needs to receive information about and to be able to analyse system artifacts.

Implementation of a strong responsive framework will require the development of reporting thresholds, adaptable response and recovery plans, and the necessary coordination, information sharing and incident reporting mechanisms needed for those plans to succeed.

4.3 – Security quality management services

Security quality management services relate to the security management processes of the constituents, particularly where national / governmental CERTs can provide specific and consistent support in, for example, security awareness building, CIIP business continuity or risk analysis. Because of its unique position and mandate, a national / governmental CERT is very well placed to provide related services to its constituency:

The national / governmental CERT can use and aggregate the output of the reactive and proactive services it delivers for all its constituents regarding, for example, the most frequently reported incidents and newly discovered vulnerabilities. It also has (at least part of) the cyber-security expertise in-house (incident handlers and technical experts) to provide services or support regarding security quality management (where normal companies may need to hire external consultants). In its role as CERT-of-last-resort and mandate as the official national point of contact, the national / governmental CERT has the authority and the breadth to reach all relevant domestic organisations and the country's population.

The most important security quality management services that should be considered for delivery by national / governmental CERTs are the following.

- Awareness building: the national / governmental CERT has an important role in advancing security knowledge and awareness, both within government and critical information infrastructure organisations, as well as with the general public. Most CERTs publicise awareness materials with regards to, for example, password best practices and phishing protection. As humans are often considered one of the weakest links in cyber-security, awareness building is a very important objective.
- Education and training: during workshops, courses, tutorials or exercises, national / governmental CERTs may provide their constituents with information and training on various topics, such as good practices in incident or vulnerability management. More and more national / governmental CERTs will organize national exercises to train their staff and key constituents, often in collaboration with a military CERT.
- Business continuity management and disaster recovery planning: BCM/DRP is, without a doubt, a key aspect of any plan for critical information infrastructure protection. National / governmental CERT experts should be involved in the cyber-security aspects of the business continuity and disaster recovery management processes for their constituents (for, in particular, the critical information infrastructure).
- Risk management: traditional static risk analysis is now evolving towards a more dynamic process. Using their knowledge of the environments and information collected via the reactive (incident, vulnerability and artifact handling) and proactive (intrusion detection service and security assessments) services, a national / governmental CERT can build a snapshot of the situational awareness in its constituency. This snapshot of overall risk will support decision-making in situations where a significant incident or crisis has arisen.

Recommendations:

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


SERVICE
PORTFOLIO
OPERATION
MANDATE
& STRATEGY
OPERATION
OPERATION

5 – Operation

Policy- and decision-makers must recognise that, in order to implement and operate a national / governmental CERT capability, there is a vast need for appropriate people, technology and processes. Without operational resources such as staff and infrastructure, a national / governmental CERT cannot offer the services discussed in the previous chapter. In this chapter, the business case for the required operational needs such as staff and infrastructure is developed. The operational capabilities and requirements that enable a national / governmental CERT to provide services of adequate quality to its constituency are also discussed.

In certain cases, the operational requirements for national / governmental CERTs are very different from those of private or academic CERTs. National / governmental CERTs have a unique coordinating role in times of national crises that affect national information infrastructures such as public communications networks or financial services. Because of this function, a national / governmental CERT will be required to continue operating under all circumstances. As a result, business continuity is of the utmost importance. In comparison, the requirements for continuity of most private or research organisation CERTs will be linked to their host organizations.

The chapter will cover the following four essential operational aspects:

- human resources
- infrastructure
- service delivery
- business continuity.

5.1 – Human resources

Human resources requirements will of course depend on several factors such as the mandate assigned to the national / governmental CERT, regulatory and business drivers, the size of the country, business hours, etc.

Team

In European Union Member States, national / governmental CERTs are normally organized in a central team structure. Larger countries could choose to use an organizational model with local teams in each state, province, department or region (as is done, for example, in India). The most important roles in a national / governmental CERT team are:

- Team leader / manager / coordinator who:
  - provides strategic direction;
  - is the authoritative representative of the national / governmental CERT
  - supervises or leads the team.
- Incident handlers who:
  - provide incident handling capability by monitoring, analyzing and responding to incidents;
  - Undertake technology watch, the dissemination of information and other tasks when no incidents are ongoing.
- Technical experts who can take on a number of roles, such as:
  - vulnerability handling;
  - technical writing;
  - training;
  - platform specific support.
- Support staff who:
  - carry out administrative tasks;
  - monitor reports on events and incidents;
  - undertake technology watch and the dissemination of information.

Without a team leader and at least one incident handler, a national / governmental CERT could not exist. But it is difficult to provide sensible requirements for the (initial) size of a national / governmental CERT, as various factors influence the number of staff. And, in many cases, funding restrictions prove one of the biggest limiting factors.

Staff skill is a very important aspect for a national / governmental CERT, as the quality of service will depend greatly on the personal and technical skills of the staff. Communication skills and cyber-security knowledge are the most essential competences of a national / governmental CERT employee.

Operation mode

The absolute minimum size for a national / governmental CERT is three FTEs (full time equivalents). With three staff, an office-hours service can be delivered. However 100% availability will not be attained. International cooperation and timely incident response will prove a challenge because of time differences and the lack of 24/7 availability. To provide one 24/7 work-shift, at least five staff members are required. The main service that warrants a 24/7 shift is the incident handling service. Incidents in critical information infrastructure may not wait until the morning to be resolved, as the consequences could be catastrophic.

As a national / governmental CERT is both working for the protection of the critical infrastructure of a government and usually acts as a CERT-of-last-resort for all incidents in its constituency, it should be considered mandatory for the CERT to be reachable 24/7/365 by its constituents and its national and international partners. To provide such a service, an estimated six to eight members of staff are required as a minimum.

Depending on the service portfolio, work structure and responsibilities, the team will need to be reachable either physically or through 'on-call duty'. In any case, it is crucial to guarantee quick response times, especially for incident reports, the core CERT service. Depending on the service portfolio and the CERT's responsibilities, a number of specialized technical experts will need to be included in the team, in order to provide, for example, artifact handling and security assessment services.

Where shift work or on-call duty schedules are used, special procedures and requirements, such as escalation procedures, maximum response times, backups, etc, must be established.

Recommendations:

- *Adequate and appropriate human resources should be dedicated to supporting the operation of the national / governmental CERT. To provide an acceptable level of service (including being reachable 24/7/365 for incident handling), national / governmental CERTs that are just starting up should strive to have a minimum of six to eight FTEs. However, periodic assessments of the appropriate staffing level, based on the size of the constituency and the breadth of services offered, are necessary.*
- *The human resources that are dedicated to the CERT need to have appropriate skills and expertise, which requires adequate investment. A profile of the staff required would include a team leader, several incident handlers and several technical experts.*

5.2 – Infrastructure

The requirements concerning confidentiality, integrity and availability of the infrastructure for national / governmental CERTs are very stringent because of:

- the role national / governmental CERTs play in crisis situations (eg, large-scale cyber-attacks);
- the confidentiality of the information processed and stored by a national / governmental CERT (records of incidents, CII vulnerabilities, etc);
- the criticality of the infrastructure that a national / governmental CERT helps to protect (energy, healthcare, communication networks, etc).

Communication services

As most national / governmental CERTs do not have direct access to the systems affected by an incident, the team will rely on its communication services to receive information about the incident in order to analyze it and to coordinate the handling of the incident. This reliance on communication services is true for almost all services a national / governmental CERT can offer.

A telephone and an Internet connection (for VOIP, e-mail and web) are the minimal set of communication equipment required and will be the most used tools. In order to exchange information securely, the national / governmental CERT should provide the contact details for signed and encrypted e-mail (eg, PGP key). In addition, the team's website should provide a secure means of communication (eg, an https-protected incident reporting form).

No single means of communications has guaranteed availability; redundancy in communication channels should always be available and announced. If possible, different means of communications should not be run over the same physical carriers, in order to avoid single points of failure in the communication infrastructure.

Logical security

Due to the sensitive nature of incidents and vulnerabilities, national / governmental CERTs process and store a large amount of confidential information. In addition to security measures for the communication channels, logical security controls should be implemented to protect the confidentiality and integrity of information, by means of, for example:

- An internal information security management framework and policy – in order to provide the security strategy and authorization to implement controls over the:
  - information classification scheme, shared with the constituency and partners in cooperation;
  - password policy;
  - access management policy;
  - etc;
- Integrity controls (eg, hash comparison) to prevent unauthorized changes;
- Confidentiality controls such as encryption.

Additionally, all logical security measures should be managed by the national / governmental CERT itself, in order to ensure confidentiality and integrity.

Physical security

An often underestimated factor is physical security. As a national / governmental CERT naturally deals with sensitive information that needs to be protected, adequate measures must be taken to physically secure the premises of a team. This is even more important considering that a national / governmental CERT not only processes information from its own country but also sensitive information from other countries that is shared with the team.

Recommendations:

- *The national / governmental CERT should ensure high availability of their communications services by avoiding single points of failure and have at least several means for being contacted and for contacting others. Furthermore, the communication channels should be clearly specified and well known to the constituency and cooperative partners.*
- *Security measures to ensure the confidentiality and integrity of information in transit (secure e-mail, https) and at rest (encryption, access control) should be implemented and managed by the national / governmental CERT.*
- *The national / governmental CERT should be secure in every way, not only logically but also in the physical sense. The offices and the supporting information systems must be located in secure sites.*

5.3 – Provision of services

For every external service delivery organisation, the efficiency and effectiveness of the service it delivers is of major importance. The national / governmental CERT should identify and monitor their most important key performance indicators (KPI) in order to evaluate the quality and performance of their services. The indicators should be relevant to the national / governmental CERT's key mission objectives and weighted according to the importance of the services to which they relate.

Examples of various quality parameters can be found in reports [2] or frameworks for information security metrics [3] [32]. The general KPI are:

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

As examples:

- Follow-up time on vulnerability reports for all non-urgent vulnerabilities: the national / governmental CERT will follow-up with a constituent within two working days of the initial report.
- Follow up on high-priority incidents: every high-priority incident will be acknowledged within two hours. Analysis will start within the first hour of receipt of such a report.

Several supporting processes and tools could increase the efficiency and maturity of service delivery.

A mandatory tool for service delivery is an incident recording and tracking system (aka a ticketing system). This will allow the creation of tickets that are associated with incidents. During the incident handling phases the ticket will be enriched with information, ensuring a formal audit trail and log of the incident.

The definition of standard procedures within the services rendered by the national / governmental CERT will ensure that processes are executed. These procedures are also the keys to the provision of a maximised level of effectiveness by a national / governmental CERT.

In terms of supporting technology, a workflow management system can queue and centralize information coming in via different communications channels, and it allows for predefined workflows to be followed in the handling of incidents. This allows proper monitoring of the status of various incidents, facilitates the hand-over between shifts, generates reports, ensures standard processes are followed, etc. Ideally the service delivery will be defined in an SLA along with the cost. At the very least, the team needs to publish the most important KPI.

Recommendations:

- *A service management quality system should be created to follow-up on the performance of the national / governmental CERT and ensure a continuous process of improvement. This could be based on clearly defined metrics that include formal service levels and key performance indicators.*
- *In order to increase the efficiency and effectiveness of the services of the national / governmental CERT, supporting processes and procedures should be defined and supporting tools should be implemented.*

5.4 – Business continuity

A national / governmental CERT is involved in the mitigation of targeted attacks against the infrastructure of its country. Therefore, the resilience of the team's infrastructure in the face of attacks needs to be ensured, as well as its possession of a solid plan for service continuity. Having and demonstrating this ability also directly reflects on the perceived competence and level of trust its constituency has in a team.

Ensuring continuity is a more general issue covering many important aspects of operations.

Managing incoming requests and the ability to correctly distribute them between staff (even across work-shifts) is one of these aspects. A second is the 24/7/365 operational mode which allows constituents to call in reports anytime (see paragraph 5.1). A third aspect is the ability to cope with the unavailability of critical communication channels and operational elements such as e-mail or information servers (WWW, FTP, etc). This could lead to an inability to provide specific services in a timely fashion and failure to meet contractual requirements and/or services as specified in service level agreements. This needs to be avoided as far as possible by a redundant and resilient infrastructure and a variety of communication channels as discussed previously.

Other important topics are the ongoing training of staff to ensure that they possess up-to-date knowledge (an investment in continuity in the longer term) and regular exercises.

Recommendations:

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


SERVICE
PORTFOLIO
COOPERATION
MANDATE
& STRATEGY
OPERATION
COOPERATION

6 – Cooperation

The security and resilience of national cyber-infrastructure is the joint responsibility of all stakeholders, including operators, service providers, hardware and software providers, end-users, public bodies and national governments. These organisations each have their own roles to play in implementing and operating the national and governmental cyber-security strategy, and in order to be effective they must cooperate closely.

If national / governmental CERTs are to meet their objectives, sustained and effective cooperation at both the national and international levels is indispensible. Threats, vulnerabilities and subsequent incidents in cyber-space often affect more than one sector or country. Therefore, there is a special need for cooperation during times of emergency.

The European Council recognises the need for a collaborative European approach to Network and Information Security in the international arena as it is a global challenge.

Council Resolution on a collaborative European approach to Network and Information Security - 2009/C 321/01

In Europe, a number of national / governmental CERTs have already established relationships with other national / governmental CERTs and with national and international CERT associations and have reached a significant level of maturity, producing high quality responses and information. They have also made bilateral agreements within certain groups on the use of common procedures, terminology, frameworks, standards, etc. Yet a large gap still remains; certain national / governmental CERTs currently lack the maturity or resources to reach these levels of cooperation. In the field, this gap translates into a number of difficulties in cooperation, for example:

- An effective coordinated response is not possible when an incident report is passed on to a neighbouring national / governmental CERT and that CERT does not act upon it by taking the necessary measures.
- If procedures differ too much between various national / governmental CERTs, cooperation will prove to be problematic in practice.

Different situations require different models of cooperation. A national / governmental CERT will use different procedures to cooperate with a domestic law enforcement organisation or telecom operator than it will use to cooperate with another national / governmental CERT on the other side of the globe. The most important cooperation models are bi/multi-lateral cooperation and an association or community.

- Bi/multilateral cooperation: bi/multilateral cooperation is a model of cooperation between two or more teams or organisations that is based on lateral agreements, ie, agreements between the parties without a group or association being formed. The agreement could be informal (ie, solely based on trust) or it could be formalized by a mandate, a non-disclosure agreement (NDA), a memorandum of understanding (MoU) or a contract.
- Association or community: an association or community is a model of cooperation between many teams or organisations which have common interests and objectives. The framework for this kind of cooperation might be set by a common geographical area, common sets of services, similar constituencies or sectors of operations, etc.

In the following subsections, a number of policy recommendations are highlighted for national and cross-border cooperation, in order to help improve national / governmental CERTs and ensure better cooperation in the future.

For more information, reference should be made to the ENISA publication CERT cooperation and its further facilitation by relevant stakeholders **[11]**.

6.1 – National cooperation

On a national level, national / governmental CERTs cooperate with numerous organisations, first and foremost with their constituencies. And, depending on the country, a national / governmental CERT will also have cooperative relationships with stakeholders such as law enforcement agencies, the military and intelligence community, policymakers, other CERTs, etc.

Constituency

A CERT's cooperation with its constituency is defined by the services that it delivers, as discussed in section 4 – Service Portfolio.

The authority that a national / governmental CERT has over its constituency depends on the mandate it has received from its government and defines how the CERT will be able to interact with its constituents. In most cases, a 'voluntary model' is applied, ie, the national / governmental CERT does not have the authority to enforce actions upon its constituents and is dependent on their willingness to cooperate. In certain cases, however, the national / governmental CERT has been given authority over its constituency, though this authority is often only valid in a time of crisis and is limited in scope.

Whether the regulated model or the voluntary model is preferable is open to debate. Both models have their advantages and disadvantages. In the voluntary model, the national / governmental CERT is powerless if a constituent refuses to act on its advice. However, when the national / governmental CERT decides on the measures to be taken and enforces them, the CERT will become liable for those actions. The authority in the regulated model should, in any case, be limited. A national / governmental CERT does not need access to its constituents' systems, for example.

Regulation? [1]

What to regulate and what not to regulate is always a subject of dispute among the parties concerned. Better cooperation is without a doubt beneficial for all parties involved. However, efforts should be directed at convincing rather than forcing cooperation, as this model has proved very successful in the past.

Of course, wherever a close relationship between CERT cooperation and public safety exists, at least some regulation should be applied. Public safety involves the protection of the general body of citizens from all kinds of significant danger, injury, damage or harm, such as may occur in a natural disaster, and the prevention of such events. Although this protection is provided by those traditional organisations known as emergency services (police, fire and rescue, and ambulance services), in the preventative sense public safety must be the priority for all those who, in any way, engineer circumstances for others.

It may be worthwhile to think about extending the definition of public safety to internet and NIS related issues.

[1] http://www.enisa.europa.eu/act/cert/background/coop

Recommendations:

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

Internet service providers / telecommunication network operators

As CII operators, internet service providers (ISPs) and telecommunication network operators are members of the constituency of national / governmental CERTs, but they play a special role as operators of infrastructure on which various stakeholders rely on.

When dealing with large-scale incidents at a national level, internet service providers and public telecommunication network operators are an important part of the puzzle. Their cooperation is needed in order to effectively handle network security incidents on a national or international scale. The best way to handle a distributed denial of service attack, a massive worm outbreak or a botnet command and control server takedown is through close coordination and cooperation with ISPs and telecommunication network operators.

Over the last few years there has been a shift in the way clients, who are unknowingly involved in unauthorized activities from their networks, are handled towards a more proactive response to these incidents and the actions taken to counter them in, for example, the case of malware. Recently there have been several initiatives to take active measures against customers whose systems are part of an ongoing security incident and who do not follow the guidelines to implement the necessary security measures. A recent example is the 'icode', a voluntary code of practice created by the Australian Internet Industry Association. This code recognises that both (ISPs) and consumers can and must share responsibility for minimising the risks inherent in using the internet. [4]

Recommendations:

- *In line with their mandates, national / governmental CERTs should establish particular cooperative relationships and procedures with internet service providers and telecommunication network operators. These, typically private, companies play a key role in the handling of large-scale incidents and are part of the national critical information infrastructure.*
- *Where a national internet service providers' or telecommunication network operators' community exists, national / governmental CERTs should consider being involved in the community or in a relevant working group (eg, a security workgroup). Where such a community or group does not exist, the national / governmental CERT should consider organizing a cooperative community with the internet service providers and telecommunication network operators.*

Other CII operators

The importance of critical information infrastructure for Europe and its Member States has been highlighted many times in recent communications and directives from the European Commission. The EC communication on CIIP Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience **[16]** refers to challenges such as insufficient coordination and cooperation.

In dealing with the challenges to CIIP, the national / governmental CERT plays an important part as it is well placed to be involved and take a leading role in the coordination and cooperation required to protect critical information infrastructure – in the crisis situation when an incident is ongoing, and in the preparation phase when critical infrastructure is being readied, as well as in the post-mortem stage when the lessons learnt after an incident or crisis are being processed.

Recommendations:

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

4 http://www.iia.net.au/index.php/codes-of-practice/icode-iias-esecurity-code.html

Law enforcement

Cooperation with law enforcement agencies is an important aspect of the handling of incident reports concerning, for example, botnet activity or illegal website content. If the organisation hosting the system does not react to an informal cease-and-desist request, a law enforcement agency will typically have to be engaged in order to take those systems or websites down. However, the process does not stop when the systems or content have been taken down. The goal in the end is to stop the criminal behind the illegal activities. In order to reach that goal, a well-functioning (and legal) information exchange and collaborative process between the national / governmental CERT and law enforcement agencies is of crucial importance.

Stopping cyber-criminals is increasingly becoming a priority, as the cyber-crime economy continues to grow. In recent years, cyber-crime has become a complex, professional and very lucrative business. Cyber-criminals have developed business models around malware packages and have increasingly professionalised the development of malware.

Cooperation with law enforcement can work in both directions. National / governmental CERTs will contact a law enforcement agency when they encounter criminal activity while handling an incident. However national / governmental CERTs also have very valuable information, knowledge and connections to offer to law enforcement agencies:

- The incident data collected by national / governmental CERTs may contain information on criminal activities on the internet.
- As part of their day-to-day job, incident handlers of national / governmental CERTs gather a vast knowledge base on the activities, tools and techniques of cyber-criminals.
- National / governmental CERTs cooperate daily with many organisations at the national and cross-border level. As a result, national / governmental CERTs are well connected in the cyber-security community.
- Some national / governmental CERTs offer specific services and therefore many have in-depth knowledge in computer forensics and artifact analysis.

Because law enforcement agencies are typically bound by more stringent rules than national / governmental CERTs, due care and consideration must be given to the regulations that govern police investigations. Law enforcement agencies may not be able to accept or share information as freely as CERTs. Therefore a formal and legal framework for cooperation should be developed in order to always ensure adherence to the regulations and investigative rules that are inherent with law enforcement activities.

Furthermore, where the national law enforcement authorities do not have adequate technical capabilities in cyber-security, the national / governmental CERT may be able to assist with detailed technical expertise.

Besides national law enforcement agencies, national / governmental CERTs may also come into contact with European or international law enforcement agencies such as Europol or Interpol, either directly or through their national law enforcement agency. Where there is frequent contact, procedures may be developed to support and streamline the process involved. However, when there is rarely any contact, it may be better to route the contact process through the national law enforcement agency, as they will have standard procedures in place to cooperate with European or international law enforcement agencies.

Recommendations:

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

Policymakers

When a national cyber-security coordination centre exists, it is often responsible for providing technical and strategic advice on cyber-security matters to policymakers. However, where such a national strategic centre has not been created by the government, a national / governmental CERT is well placed to provide technical and strategic advice to policymakers in the government.

Recommendations:

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

Other CERTs

National / governmental CERTs should cooperate with other domestic CERTs, where their role is that of a CERT-of-last-resort. In this case, the national / governmental CERT must forward incident reports to the appropriate domestic CERT when the reporting entity is part of the constituency of another domestic CERT. Because of its particular role in critical information infrastructure protection, a national / governmental CERT should have strong working relationships with the CERTs of the operators of critical information infrastructure.

Furthermore, when a significant national incident in cyberspace occurs, the national / governmental CERT will, at the very least, play a coordinating role in the handling of the incident. The organisations or sectors a particular incident may affect cannot be foreseen beforehand. In order to be prepared for this uncertainty, the national / governmental CERT should strive to have cooperative relationships in place with as many domestic CERTs or other incident management teams as is feasible.

In any case, a national / governmental CERT should have cooperative relationships with at least a significant part of the national incident response or CERT community. Through these relationships, the team will be well-placed to organize a community or working group for domestic CERTs.

Recommendations:

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

Military and intelligence

The cooperation between the military or intelligence community (eg, military or department of defence CERT) and national / governmental CERTs has two dimensions: peacetime and wartime cooperation. Cyberwarfare has been a much debated topic in recent years, and yet the same, difficult questions remain: How can cyberwar be defined exactly? What constitutes an 'act of war' in cyberspace? To whom do you attribute a cyber-attack? Currently, no generally accepted answers to these questions exist in the international community. However, recent cases have illustrated a convergence between military actions in the physical and cyber-domains.

What is not under discussion is the fact that both military CERTs and national / governmental CERTs can benefit mutually through cooperation; for example:

- Sharing incident data can greatly improve the capabilities of the national / governmental CERT and the military/intelligence communities concerning their awareness of the national situation.
- National / governmental CERTs can benefit from the unique positions of military and intelligence agencies, as these agencies are often preferred targets of attacks.
- In most cases, military and intelligence agencies depend on critical civilian information infrastructures (mainly energy and communication infrastructures).
- Both communities have developed good practices in various areas from which the other community can benefit.

During peacetime, cooperation is similar to cooperation with other national / governmental CERTs, though it includes some additional benefits (as discussed in the above examples). During times of crises additional capabilities in coordination would be necessary to efficiently and effectively mitigate and repulse a cyber-attack.

However cooperation between both communities is not straightforward. Military and intelligence communities often cannot share attack and incident information because such data is classified as secret and due to the constraints of 'need to know'. Common problems with classified data are that the personnel in a national / governmental CERT do not have the necessary security clearance or an appropriately cleared communication channel between the two parties is not available.

Recommendations:

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

6.2 – Cross-border cooperation

In their roles of as national points of contact for foreign CERTs, national / governmental CERTs will cooperate with foreign teams on a daily basis, most commonly with their peers in other countries.

The most important factor for success as a national point of contact is trust. If the national / governmental CERT has not established and does not actively maintain its trustworthiness, constituents and other CERTs may hesitate to contact the team, might bypass it and might exclude the CERT from information sharing or other forms of collaboration.

Recommendations:

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

Initiatives in cooperation

Initiatives in European and international cooperation are mainly focused on the following aspects of CERT activities: trust building, sharing knowledge and information (collaboration), and preparing for cross-border coordination during incidents.

However, cooperation among CERTs has proved to be most effective within regions. This can be easily explained by the fact that short travel times and relatively low costs overall stimulate more frequent personal meetings. Another important reason is that the similarity in cultural backgrounds and the common native language of the participating teams makes social networking easier and facilitates common projects. Some of the longest standing and most mature initiatives in regional cooperation have been developed in Europe.

Some of the most important networks and centres for cooperation at the European level are (in no particular order):

TF-CSIRT

Terena (Trans European Research and Education Networking Association) TF-CSIRT[5] is a task force that promotes collaboration between CERTs at the European level and liaises with similar groups in other regions. The TF-CSIRT meets on a regular basis at locations all over Europe.

5 http://www.terena.org/activities/tf-csirt/

TF-CSIRT provides a forum where members of the CERT community can exchange experiences and knowledge in a trusted environment. Participants in TF-CSIRT are actively involved in establishing and operating CERT services in Europe and in neighbouring countries.

The task force promotes the use of common standards and procedures for responding to computer security incidents. Common standards have great potential for reducing the time needed to recognise and analyse incidents, and then take appropriate countermeasures.

The task force also assists with the establishment of new teams, and trains the members of existing teams in the latest incident handling tools and techniques.

Trusted Introducer (TI)

The Trusted Introducer (TI[6]) is a trust broker for European CERTs. The 'web-of-trust' is built on three levels:

- listed – any team identified as being within the scope of TI;
- accreditation candidate – a team which has received and accepted an invitation to the accreditation process;
- accredited – a team which has successfully completed the accreditation and verification process.

An invitation to start the accreditation process can be sent to a 'listed' team on its own request or as a result of a recommendation from an already 'accredited' CERT. The process of accreditation requires the team to declare its support for a number of criteria and provide a standardized set of information about itself. This data is then kept and maintained by the TI to ensure it is correct and up to date. Gaining the 'accredited' level results in access to numerous services, eg, a database of in-depth operational contacts of all accredited teams, the TI mailing lists open to accredited CERTs only, PGP key signing, etc.

European Network and Information Security Agency (ENISA)

ENISA is a centre of excellence in network and information security for European Union Member States and European institutions. It provides advice and recommendations, and acts as a switchboard of information about good practices in NIS. In addition, the agency facilitates contacts between European institutions, the Member States and the private sector.

ENISA is currently administering several initiatives in cooperation:

- The Clearing House for Incident Handling Tools (CHIHT), a TF-CSIRT project, is hosted by ENISA. It consists of a list of software packages useful in everyday CERT activities, based on input from CERT teams of the task force.
- ENISA organizes its CERT in Europe workshops[7] on a regular basis (often adjacent to a TF-CSIRT meeting). The workshop presentations focus on improving cooperation and coordination among European CERTs, and provide an overview of running initiatives, new topics, ongoing research, etc.
- Since its inception, ENISA has published numerous reports, guidelines, training materials and best practices guides with regards to the full range of CERT services and related areas[8].

Some of the most important initiatives in cooperation at the international level are (in no particular order):

FIRST

FIRST is the major international forum for CERTs and other security teams. FIRST brings together more than 200 members from around the world. The mission statement of FIRST is:

- FIRST is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs;
- FIRST members develop and share technical information, tools, methodologies, processes and best practices;

6 http://www.trusted-introducer.org/
7 http://www.enisa.europa.eu/act/cert/events
8 http://www.enisa.europa.eu/act/cert

- FIRST encourages and promotes the development of quality security products, policies & services;
- FIRST develops and promulgates computer security best practices;
- FIRST promotes the creation and expansion of Incident Response teams and membership from organisations from around the world;
- FIRST members use their combined knowledge, skills and experience to promote a safer and more secure global electronic environment.

Within the forum there are many formal and informal groups that are usually based on common areas of interest, constituencies or provided services. Formal cooperation is built within the confines of SIGs (special interest groups). The SIGs exist to provide forums where FIRST Members can discuss topics of common interest to the incident response community. A SIG is a group of individuals composed of FIRST members and invited parties, typically coming together to explore an area of interest or specific area of technology, with the goal of collaborating and sharing expertise and experiences to address common challenges.

For better coordination and to give members a chance to participate more often in the organisation's meetings, a closer coordination with regional forums has been established. For example, the collocation of FIRST and TF-CSIRT meetings has proved to be successful.

IMPACT

The International Multilateral Partnership Against Cyber Threats (IMPACT[9]) is a non-profit comprehensive global public-private partnership. IMPACT was founded only recently, in 2008, and is positioned to assist partner countries, with a focus on developing nations, in broadening their cyber-security capabilities and capacity. IMPACT is a politically neutral platform, bringing together governments, academia, industry leaders, international organisations, think tanks and cyber-security experts to enhance the global community's capacity to prevent, defend against and respond to cyber-threats.

In 2008, IMPACT and the ITU[10] (International Telecommunication Union) signed a memorandum of understanding (MoU) in which IMPACT's global headquarters effectively became the physical and operational home of the ITU Global Cyber security Agenda (GCA). Under this landmark collaboration, IMPACT provides ITU's 191 Member States with the expertise, facilities and resources to effectively address cyber-threats.

Recommendations:

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

Sector working groups

Another incentive to cooperate is the similarity of the sectors in which CERTs operate. A sector is mainly defined by the constituency, but also by the responsibilities of a specific CERT. A national / governmental CERT working group is an example of sectoral cooperation. Some teams associate and start closer cooperation because of a common area of interest, such as work in the same or similar type of environment. This kind of cooperation exists in the public as well as in the private sector.

Some of the most important sectoral working groups include the FIRST Special Interest Groups (SIGs)[11] and the European Government CERTs group (EGC).

European Government CERTs group (EGC)

The European Government CERTs group (EGC) is an informal group of governmental CSIRTs that is developing effective cooperation between its members on matters relating to incident response, by building on the similarities in constituencies and sets of problems among governmental CSIRTs in Europe. To achieve this goal, ECG group members:

9 http://www.impact-alliance.org/
10 http://www.itu.int/
11 http://www.first.org/global/sigs/

- jointly develop measures to deal with large-scale or regional network security incidents;
- facilitate information sharing and technology exchange relating to IT security incidents and malicious code threats and vulnerabilities;
- identify areas of specialist knowledge and expertise that could be shared within the group;
- identify areas of collaborative research and development on subjects of mutual interest;
- encourage the formation of government CSIRTs in European countries;
- communicate common views with other initiatives and organisations.

Recommendations:

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

6.3 – Crucial elements for cooperation

Trust

Trust building

Cooperation between CERTs (such as sharing information on vulnerabilities or incidents, aiding with incident response, etc) is only possible if both CERT organizations trust each other and the quality of information and service provided. As such, building trust is a very important matter if national / governmental CERTs are to cooperate on a daily basis over geographical or public-private sector borders. Trust can be built by long-standing informal working relationships or by means of more formal relationships such as bilateral or multilateral agreements, community membership, sponsorship or accreditation.

Trust models

The most basic form of trust is an informal relationship. During day-to-day operations, national / governmental CERTs will cooperate with many organisation and individuals with whom the CERT does not have any formal agreement. With recurring fruitful cooperation, a relationship based on subjective trust will be built between persons or organisations.

The most basic way to establish formal trust is by signing a legal document that contains an agreement between parties (bi/multilateral or community agreement). The document would contain the scope and nature of the agreement. In certain cases, the agreement is not legally binding, eg, a commonly used Code of Conduct (CoC).

Europeans will not embrace technology they do not trust - the digital age is neither "big brother" nor "cyber wild west".

European Commission - A Digital Agenda for Europe - COM (2010) 245

International CERT associations that provide membership on a basis of trust were created because it became impossible for any CERT to build one-to-one relationships of trust with every possible CERT with whom they might have to cooperate potentially. Most of these associations are based on a sponsorship principle: in order to join the association, one or more full members need to sponsor the application for membership. These sponsors will have existing relationships based on trust with the applicant (eg, FIRST).

When needed, a community can use a process of accreditation to establish a level of trust for its members. This process should probably be performed by an external, independent authority – a trusted third-party. The purpose of accreditation is to ensure the competence and quality of services necessary to grant a certain level of trust. An example of CERT accreditation is the Trusted Introducer (TI) accreditation for European CERTs.

Recommendations:

- *On a national level, the national / governmental CERT should build relationships of trust with domestic CERTs and other domestic organisations (eg, law enforcement agencies, national security or intelligence agencies, the operators of critical information infrastructure, etc). If necessary the national / governmental CERT should consider organizing or promoting the organization of one or several communities for cooperation with a sector specific focus or common objective.*
- *On an international level, national / governmental CERTs should engage in trust building activities and cross-border cooperation, and should consider membership of international or European CERT associations and alignment with relevant CERT accreditation schemes.*

Quality of information

The growth in digital information exchange has also increased the need for improvements in the quality of data and information. National / governmental CERTs are flooded with information from various sources and are burdened with the task of interpreting that data, filtering out the relevant information, enriching or correlating the data, and disseminating the information in a timely way to the correct target audiences or responding to the information themselves. Therefore, in order to establish efficient, effective and appropriate cooperation between national / governmental CERTs, the following characteristics of information should be considered in the interaction with relevant stakeholders:

- Relevance: national / governmental CERTs must be able to distinguish relevant from irrelevant information and select what information to share or disseminate. Based on factors such as affected systems or application name and version, constituents can then assess whether the information is relevant to their organisation.
- Completeness: if the information about an incident is incomplete, the national / governmental CERT will not be able to act upon that information, which may result in wasted resources and further escalation of an incident. To avoid incomplete information, it is advisable to adhere to standards.
- Timeliness: national / governmental CERTs often deal with very time sensitive information. Information concerning incidents and vulnerabilities affecting critical information infrastructure needs to be disseminated as fast as possible to avoid or contain incidents.

Additional important aspects related to the quality of information include:

- Security: confidentiality, integrity, availability and authenticity of information are very important, even more so at the time of an incident or crisis.
- Verifiability: if the information source is not trustworthy, the information could be fake or manipulated. The information should be verifiable and checked against multiple sources or a trusted source;
- Comprehension: shared information is useless if the other party does not understand its meaning. This subject is tackled in the following section on common terminology and schemes.

Recommendations:

- *The information that can and should be disseminated to stakeholders should be clearly defined.*
- *In order to ensure the relevance, completeness and comprehension of information in the context of cooperation with relevant stakeholders, national / governmental CERTs should define and adhere to information quality standards such as exchange and naming schemes.*
- *To ensure the security of information, national / governmental CERTs must implement security measures that ensure the confidentiality, integrity, availability and authenticity of information.*

Sustainable reaction

The main objective of a national / governmental CERT is to react to information inputs (incident reports, vulnerability reports, malware samples, etc), by coordinating a response, handling an incident, disseminating an alert, analyzing a system or vulnerability, etc.

The core and most important service that a CERT delivers is incident handling. To provide 'best practice' in incident reporting, all the elements discussed in the previous sections need to be in place:

- sufficiently high quality and timely information;
- communication and collaborative links with trusted partners;
- common terminology and schemes in use.

As well as several other building blocks discussed in other chapters, the following are also needed:

- appropriately skilled staff;
- communication and information technology infrastructure;
- 24/7 availability of core CERT services;
- sufficient mandate to enforce responses.

Only then will the national / governmental CERT be able to ensure a sustainable reaction to the information inputs it receives. For example, in an ideal case a team is able to immediately act on an incident report from another team and cut an attacking system off the network. This is only possible if the national / governmental CERT has direct access to core infrastructure such as IXPs (Internet exchange points), which is not usually the case, or has a mandate to instruct the ISPs in its country to do so. But such a mandate is not often given to national / governmental CERTs and so, again, the importance of well-functioning cooperation at the national level needs to be emphasised. Well-established cooperation among all key players in a country, such as CERTs, ISPs and other stakeholders, which is built on trust and the will to cooperate, can effectively mitigate the lack of access to core infrastructure, either directly or indirectly via mandate. A CERT that can only receive incident reports about its constituency but is not able react to them in a timely and sustainable manner cannot fulfil its obligations as a national / governmental CERT.

Recommendations:

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

Common terminology and schemes

On a national and cross-border level, a clear need exists for the definition and adoption of common standards, metrics, procedures, formats, etc, in order to facilitate information sharing and improve the interoperability, measurability and comparability of CERT activities. In terms of the incident management activities of national / governmental CERTs, this translates, for example, into the use of specific:

- incident reporting forms and incident exchange formats;
- information classification schemes;
- system and application naming conventions;
- frameworks and taxonomies for cyber-security metrics;
- procedures to handle critical incidents and the associated expectations with regards to priority, feedback, etc.

Although generally accepted cyber-security schemes and standards are still rare and under development, several initiatives exist with regards to various aspects of cyber-security, for example:

- ENISA reports and good practice guides;
- CERT/CC reports and good practice guides;
- ITU reports and good practice guides;
- US National Institute of Standards and Technology (NIST) Special Publications;
- SCAP (Security Content Automation Protocol includes standards such as CVE, CVSS, CPE, MAEC), IODEF (Incident Object Description and Exchange Format), IDMEF (Intrusion Detection Message Exchange Format), CAPEC (Common Attack Pattern), etc.

However most of these developments still lack general adoption, typically due to a lack of tools and inconsistently defined information requirements across countries and sectors.

It is clear that the use of common terms and schemes would greatly improve capabilities in cooperation as well as the quality of information. Currently, there is still a great diversity in the incident management schemes and processes among national / governmental CERTs, which results in problems with cooperation and diversity in the quality of information. If, for example, standard reporting and exchange formats were used to describe incidents, then less experienced and mature national / governmental CERTs could deliver information of a minimal quality standard, based on the format requirements.

In order to enable transparent and uniform reporting of cyber-security statistics, there is a need to invest in the development and adoption of standard frameworks for cyber-security metrics.

Recommendations:

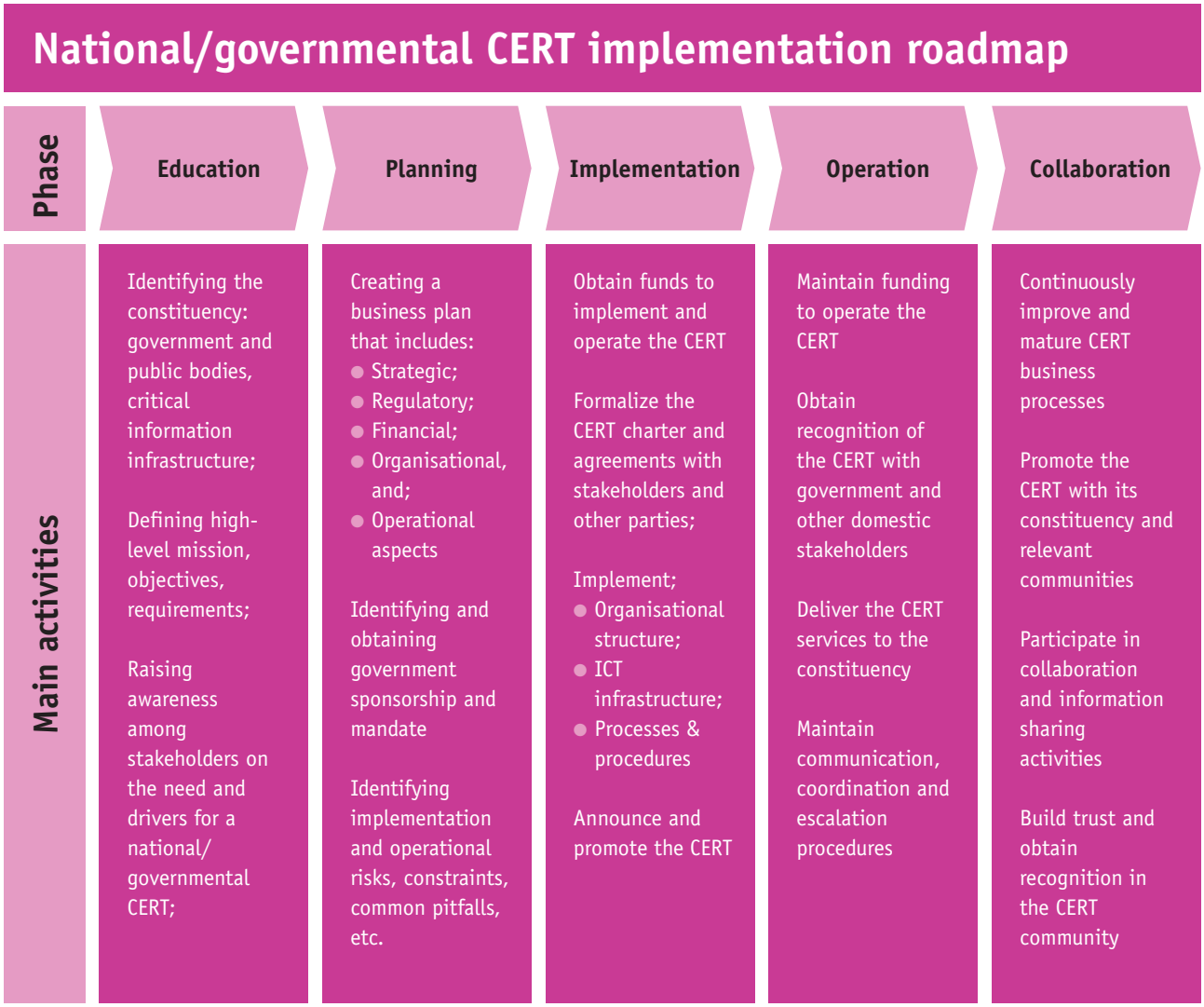
- *To facilitate national / governmental CERTs cooperation, the adoption and use of common or standardised practices should be promoted for:*
  - *incident and vulnerability handling procedures;*
  - *incident, vulnerability and information classification schemes;*
  - *taxonomies for metrics;*
  - *information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

ANNEXES

7 – Annexes

7.1 – Annex A – National / governmental CERT implementation roadmap

The diagram below shows a roadmap for the implementation of a high-level national / governmental CERT. The roadmap is mainly based on two documents: ENISA Baseline capabilities for national / governmental CERTs [10] and CMU SEI CERT/CC Steps for Creating National CSIRTs [4]. It briefly describes the activities performed within the five phases of the lifecycle of a national / governmental CERT as defined by CERT/CC: education, planning, implementation, operation, and collaboration.



7.2 – Annex B – National / governmental CERT capability maturity model

The table below provides an initial proposal for a maturity model for the capabilities of national / governmental CERTs. The model is based on experiences and observations in the field, including observations of the maturity of national / governmental and other CERTs. In addition, the maturity model levels are based on the Software Capability Maturity Model (CMM) levels defined by the Carnegie Melon University Software Engineering Institute [5].

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 is recognized as national Point of Contact in the international CERT community • Sets of defined and documented standard processes are established and maintained for core CERT services. These processes provide consistent results and process performance • Additional added value CERT services are repeatable and provide consistent 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 recoginition 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

7.3 – Annex C – References

[1] Carnegie Mellon University SEI - CERT Coordination Center (August 19, 2010) Establishing a National Computer Security Incident Response Team (CSIRT), Podcast

[2] Carnegie Mellon University SEI - CERT Coordination Center (2003) Handbook for Computer Security Incident Response Teams (CSIRTs) [Online] **http://www.sei.cmu.edu/library/abstracts/reports/03hb002.cfm**

[3] Carnegie Mellon University SEI - CERT Coordination Center (2007) Incident Management Capability Metrics Version 0.1. [Online]. **http://www.cert.org/archive/pdf/07tr008.pdf**

[4] Carnegie Mellon University SEI - CERT Coordination Center (2004) Steps for Creating National CSIRTs. [Online]. **http://www.cert.org/archive/pdf/NationalCSIRTs.pdf**

[5] Carnegie Mellon University Software Engineering Institute (1993) Capability Maturity Model for Software (Version 1.1)

[6] Center for Security Studies, ETH Zurich (2007) A Generic National Framework For Critical Information Infrastructure Protection (CIIP)

[7] Center for Security Studies, ETH Zurich (2008) International CIIP Handbook 2008/2009 - An inventory of 25 national and 7 international critical information infrastructure protection policies

[8] Center for Strategic and International Studies (CSIS) - Comission on Cybersecurity. (2008) Securing Cyberspace for the 44th Presidency [Online] **http://csis.org/program/commission-cybersecurity-44th-presidency**

[9] ENISA (2009) Analysis of Member States' Policies and Regulations - Policy Recommendations

[10] ENISA (2009) Baseline capabilitites for national / governmental CERTs [Online] **http://www.enisa.europa.eu/act/cert/support/baseline-capabilities**

[11] ENISA (2006) CERT cooperation and its further facilitation by relevant stakeholders [Online] **http://www.enisa.europa.eu/act/cert/background/coop**

[12] ENISA (2006/2007) EISAS – European Information Sharing and Alert System - A Feasibility Study

[13] ENISA (2010) Inventory of CERT activities in Europe

[14] European Commission (2010) A Digital Agenda for Europe (COM (2010) 245) [Online] **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF**

[15] European Commission (2009) Commission staff working document - Accompanying document to the Communication from the Commission on Critical Information Infrastructure Protection - Summary of the impact assessment (SEC/2009/0400 final) [Online] **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2009:0400:FIN:EN:PDF**

[16] European Commission (2009) Communication of the European Commission on Critical Information Infrastructure Protection - Protecting Europe from large scale cyberattacks and disruptions: enhancing preparedness, security and resilience (COM(2009)149) [Online] **http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF**

[17] European Commission EU policy on Critical Information Infrastructure Protection – CIIP [Online] **http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm**

[18] European Commission European Union Ministerial Conference on Critical Information Infrastructure Protection - Conference Conclusions, Talinn, 27-28 April 2009

[19] European Commission (2009) Public Consultation - Towards a strengthened Network and Information Security Policy in Europe [Online]
http://ec.europa.eu/information_society/policy/nis/nis_public_consultation/index_en.htm

[20] European Council (2009) Council Resolution on a collaborative European approach to Network and Information Security (2009/C 321/01)

[21] European Council (2008) Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

[22] Geneva Centre for the Democratic Control of Armed Forces (DCAF) (2010) DCAF Horizon 2015 Working Paper No 1 - Democratic governance challenges of cyber security [Online]
http://www.dcaf.ch/publications/kms/details.cfm?lng=en&id=117994&nav1=5

[23] Government of Canada (2010) Canada's Cyber Security Strategy - For a Stronger and More Prosperous Canada

[24] House of Lords - European Union Committee (2010) Protecting Europe against large-scale cyber-attacks [Online] http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68.pdf

[25] Institute for Information Infrastructure Protection (I3P) (2009) National Cyber Security Research and Development Challenges - Related to Economics, Physical Infrastructure and Human Behavior pdf [Online]
http://www.thei3p.org/docs/publications/i3pnationalcybersecurity.pdf

[26] Internet Security Alliance (2009) Social Contract 2.0: A 21st Century Program for Effective Cyber Security [Online]
https://netforum.avectra.com/temp/ClientImages/ISA/67c373ef-638c-45dc-86d0-7b15957401cc.pdf

[27] Internet Security Alliance (2008) The Cyber Security Social Contract - Policy Recommendations for the Obama Administration and 111th Congress [Online]
https://netforum.avectra.com/temp/ClientImages/ISA/fc4d0998-4486-4819-b1d7-1d9bff64ea4d.pdf

[28] IT-ISAC (2009) IT Sector Baseline Risk Assessment [Online]
http://www.it-scc.org/documents/itscc/IT_Sector_Risk_Assessment_Report_Final.pdf

[29] ITU Study Group Q22/1 (2008) Report on best practices for a national approach to cybersecurity: a management framework for organizing national cybersecurity efforts [Online]
http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf

[30] ITU-D ICT Applications and Cybersecurity Division (2007) ITU National Cybersecurity/CIIP Self-Assessment Toolkit - Background Information for National Pilot Tests [Online]
http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-self-assessment-toolkit-info.pdf

[31] National Institute of Standards and Technology (NIST) (2007) NISTIR 7359 - Information Security Guide for Government Executives [Online] http://csrc.nist.gov/publications/nistir/ir7359/NISTIR-7359.pdf

[32] The Center for Internet Security (2009) The CIS Security Metrics - Consensus Metric Definitions v1.0.0 [Online]
http://cisecurity.org/en-us/?route=downloads.show.single.metrics.100

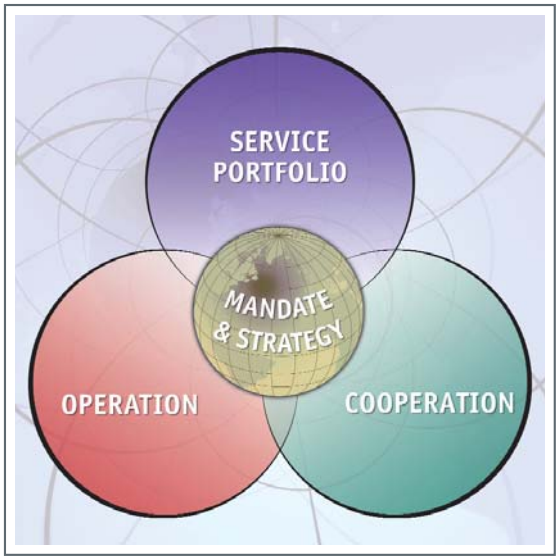
[33] The Markle Foundation Task Force on National Security in the Information Age (2009) Nation At Risk: Policy Makers Need Better Information to Protect the Country [Online]
http://www.markle.org/downloadable_assets/20090304_mtf_report.pdf

[34] UK Cabinet Office (2009) Cyber Security Strategy of the United Kingdom - safety, security and resilience in cyber space [Online] http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf

[35] UK Cabinet Office (2008) The National Security Strategy of the United Kingdom - Security in an interdependent world [Online] http://interactive.cabinetoffice.gov.uk/documents/security/national_security_strategy.pdf

[36] United Nations General Assembly (2004) Resolution 58/199 Creation of a global culture of cybersecurity and the protection of critical information infrastructures [Online] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N03/506/52/PDF/N0350652.pdf

[37] US White House (2009) Cyberspace Policy Review - Assuring a Trusted and Resilient Information and Communications Infrastructure. [Online] http://www.whitehouse.gov/cyberreview/



enisa
European Network
and Information
Security Agency

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