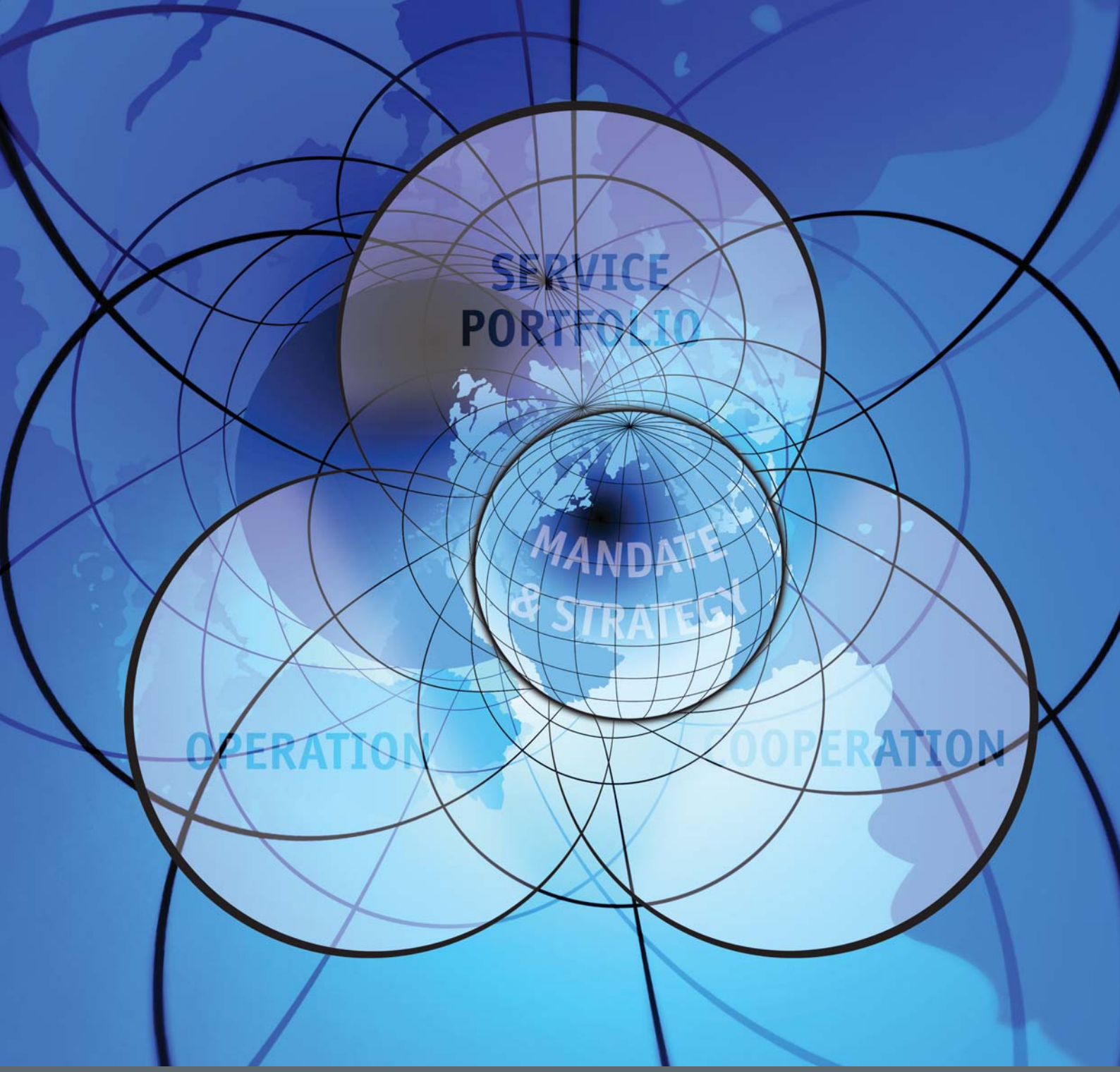


Baseline Capabilities of National / Governmental CERTs – Summary

enisa
European Network and Information Security Agency

Baseline Capabilities of National / Governmental CERTs – Summary

ENISA recognises that existing arrangements for fulfilling the responsibilities of national / governmental CERTs already operate in a number of countries and that these arrangements have often developed organically in the absence of national strategies. CERTs have taken the lead in responding to the increased threats to cyber-security and their contribution is to be valued. The recently published document *Policy Recommendations on Baseline Capabilities of National & Governmental CERTs* takes into account recommendations by internationally recognised centres of expertise and draws upon the experience and effective practice of existing CERTs.

The baseline recommendations in this document are aligned with communications from the European Council and Commission that address the challenges and priorities for network and information security (NIS) and the critical information infrastructure protection (CIIP). These are formulated in four areas: *mandate* and *strategy*, *service portfolio*, *operation* and *cooperation*.

Mandate & Strategy

Many EU Member States have recognised the need to strengthen national cyber-security including the protection of critical information infrastructure (CII) from cyber-based and other threats. Some countries have developed national cyber-security strategies and CII protection programmes. As a rule, such strategies and programmes rightly include requirements to reduce the vulnerability of critical networks to cyber-attacks, respond effectively when such attacks occur, and establish and maintain cooperative relationships with the national and international partners needed to operate effectively in the cyber domain. These are all areas of activity in which these teams play an important part. It is essential therefore that the activities of national / governmental CERTs (and those CERTs which by default have assumed a national / governmental role) are consistent with the objectives of such national strategies and programmes and complement the structures and other arrangements in order to deliver them. This requirement has a number of implications for the mandates of CERTs.

Recommendations

- *Developing a strategic approach to cyber-security and CII protection should be strongly considered. In order to avoid unnecessary duplication of effort, a national cyber-security strategy should define and mandate the roles and responsibilities of all organisations necessary for its delivery including the national / governmental CERT.*
- *The mandate for the national / governmental CERT should clearly define the scale and scope of its activities including its constituency, the nature and level of services it is required to deliver to that constituency, and its engagement in international relationships.*
- *Where the role of a national / governmental CERT has been assumed de facto by an existing body, it should be considered how best to include that CERT in the national strategy.*

Service portfolio

The service portfolio of a national / governmental CERT will be determined by its mandate and its place as part of or alongside other structures responsible for delivering the national cyber-security strategy or CII protection programme. Generally speaking, however, CERT services should reduce the vulnerability of its constituency's critical networks to cyber-attacks and support effective responses to such attacks when they do occur.

Recommendations

- *A national / governmental CERT must minimally provide its constituents with an effective incident handling capability. 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.*
- *National / governmental CERTs should also provide services to reduce the vulnerability of networks to cyber–attacks, including the analysis and disclosure of software and hardware vulnerabilities, alerts and warnings of new threats with recommendations for mitigation, and building awareness and capabilities to improve the general security posture within their constituencies.*
- *These CERTs should also provide services to support an effective response to cyber–attacks, including technical support and expertise, warnings of incidents to organisations not yet affected by them, assessments of the impacts of attacks, and communications with other national and international CERTs, and provide advice on appropriate actions, training and the conduct of exercises.*

Operation

The role and responsibility mandated for a national / governmental CERT and its service portfolio create particular requirements for its effective operation. One factor is that cyber-security incidents happen on a global scale, meaning that the team must be able to respond to incidents developing across international time zones. Another is that, both in dealing with its constituency and in its relationships with other CERTs, the national / governmental CERT must enjoy a reputation for contactability and competence in order to have the credibility which underpins its operational effectiveness.

Recommendations

- *Implementing or further developing the capabilities of a national / governmental CERT requires ensuring that it is sufficiently staffed and has at its disposal the supporting infrastructure necessary to operate around the clock. The staff must have the required technical competence to deal effectively with the members of its constituency and in other CERTs, especially when responding to incidents.*
- *Because any lapse in this would cause irrevocable damage to the credibility and authority of the national / governmental CERT, it should be provided with a secure and resilient communication and information infrastructure enabling confidential communication with other stakeholders. The CERT should also be located within physically secure premises and staff should be appropriately screened.*
- *Where the role of a national / governmental CERT is undertaken de facto by an existing body, how that CERT can be required and best enabled to meet the necessary operational needs must be considered.*

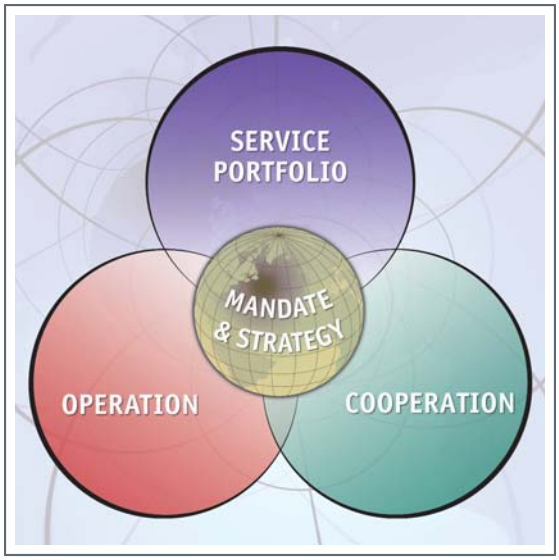
Cooperation

Threats to cyber-security and cyber-attacks on critical information infrastructures respect no organisational and territorial boundaries. For that reason, effective cooperation between CERTs at all levels is required to facilitate the exchange of the information and knowledge needed to reduce vulnerability and provide effective responses to cyber incidents. This includes CERTS within particular business sectors which might be affected by large-scale incidents, other CERTs within a country serving other communities, other national / governmental CERTs and internationally recognised research and development organisations. Because of the often sensitive nature of the information shared, effective cooperation of this nature requires trust and mutual respect between the bodies involved. It is thus inevitable that a national / governmental CERT must invest time and resources in building relationships with other CERTs and equivalent bodies on both a bilateral and multilateral basis.

Because of the nature of threats to cyber-security and cyber incidents, there might be a need for a national / governmental CERT to develop particular relations with certain communities. These include ISPs and telecom providers because of their role in operating critical information networks, military and national security agencies that might have access to relevant threat intelligence, and law enforcement agencies where criminal activity needs to be countered. Special arrangements might be needed to facilitate sensitive relationships, such as detailed memoranda of understanding, the ability to handle classified information or agreements on the initial response to reported incidents. EU Member States may have to formulate policy on such matters where they affect legal or regulatory matters or ensure that such issues are captured at a strategic level.

Recommendations

- *National / governmental CERTs should be enabled to invest time and resources in building cooperative relationships with other CERTs and similar bodies to facilitate the exchange of information and support timely responses to incidents and developing threats.*
- *Such cooperation depends on the development of trust, which requires ongoing, daily exchanges and participation in community or association based events such as conferences, seminars and exercises.*
- *Because of special circumstances, some cooperative relationships need to be underpinned by formal agreements such as memoranda of understanding or government policy. All cooperative relationships should be supported by agreement on the use and quality of shared information, a common terminology, trusted communication channels and best practices.*
- *Where the function of a national / governmental CERT is undertaken de facto by an existing body, how that body can best represent its interests in cooperating with other stakeholders should be considered.*



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