Critical Infrastructure Protection Governance: towards the implementation of best practices

Ekaterina Rudina

Critical Infrastructure Defense

KL ICS-CERT

Contents

1. Legal and regulatory landscape 2017
2. CIP governance challenges
3. Worldwide trends in security governance practices
4. What’s next

Legal and regulatory landscape 2017

- **Russian Federation: Закон о безопасности КИИ РФ** ***от 26 июля 2017 г.***

- **US S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017**

- **EU NIS Directive**
  Entry into force August 2016

- **US NIST 2017 draft Framework for Improving Critical Infrastructure Cybersecurity Version 1.1**

- **Afghanistan: Cyber Crime Code**
  Signed into Law June 20, 2017

- **China – Cybersecurity Act**
  took effect on 1 June 2017

- **Vietnam: first draft of the Law on Cybersecurity**
  published 6 June 2017

- **Singapore – Cybersecurity Bill**
  public consultation 10 July - 24 August 2017

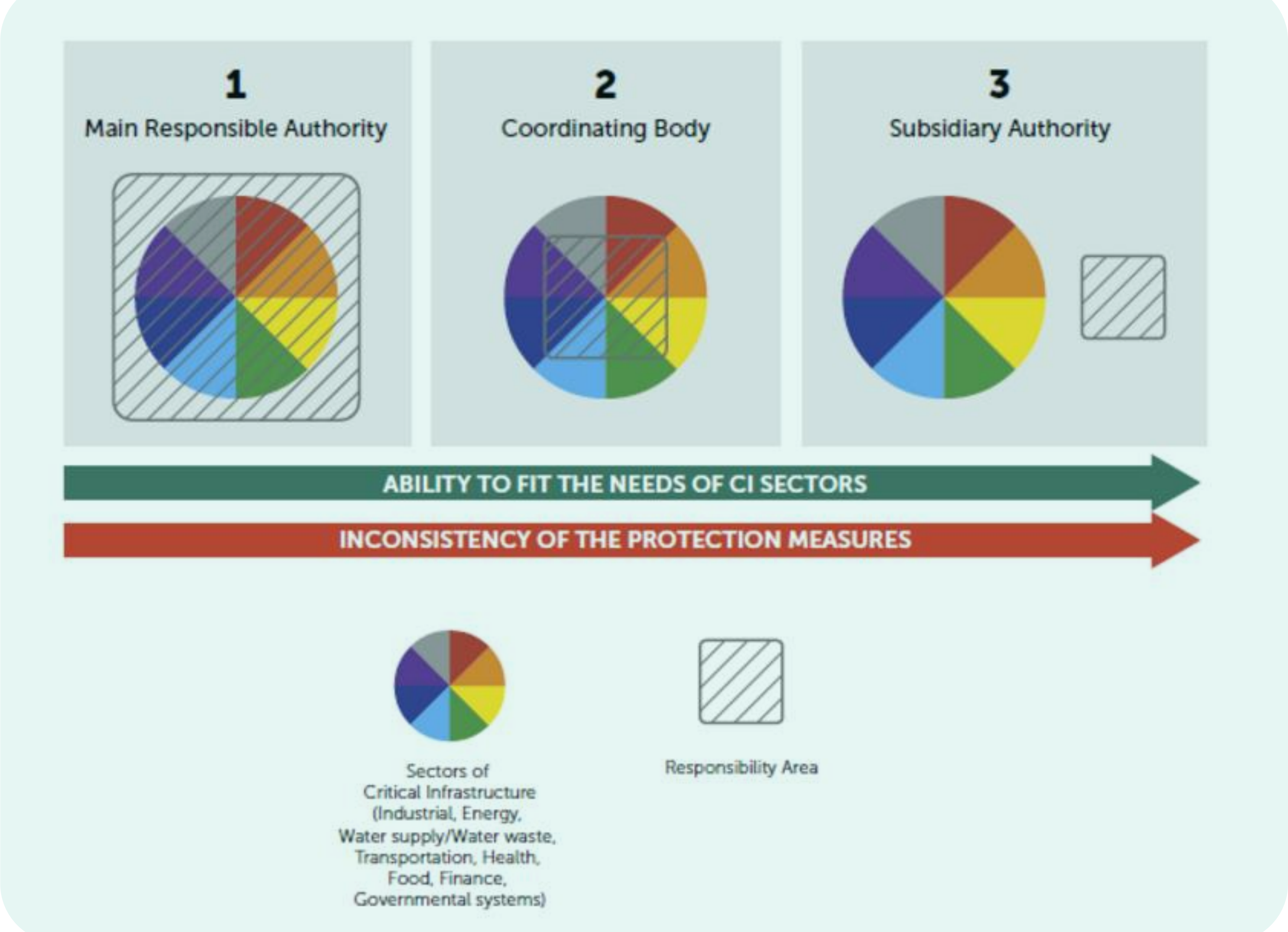
…

CIP governance challenges

- Aligning cybersecurity strategy with the national mindset
- Setting boundaries for the State interference
- Setting up the governance structure
- Identification of the CII and operators of essential services
- Distribution of responsibilities for the incident prevention and response
- Setting up a penalty regime

The most neglected

KASPERSKY lab


1
Main Responsible Authority
2
Coordinating Body
3
Subsidiary Authority
ABILITY TO FIT THE NEEDS OF CI SECTORS
INCONSISTENCY OF THE PROTECTION MEASURES
Sectors of Critical Infrastructure (Industrial, Energy, Water supply/Water waste, Transportation, Health, Food, Finance, Governmental systems)
Responsibility Area

Source: https://ics-cert.kaspersky.com/reports/2016/12/02/critical-infrastructure-protection-governance-around-the-world/

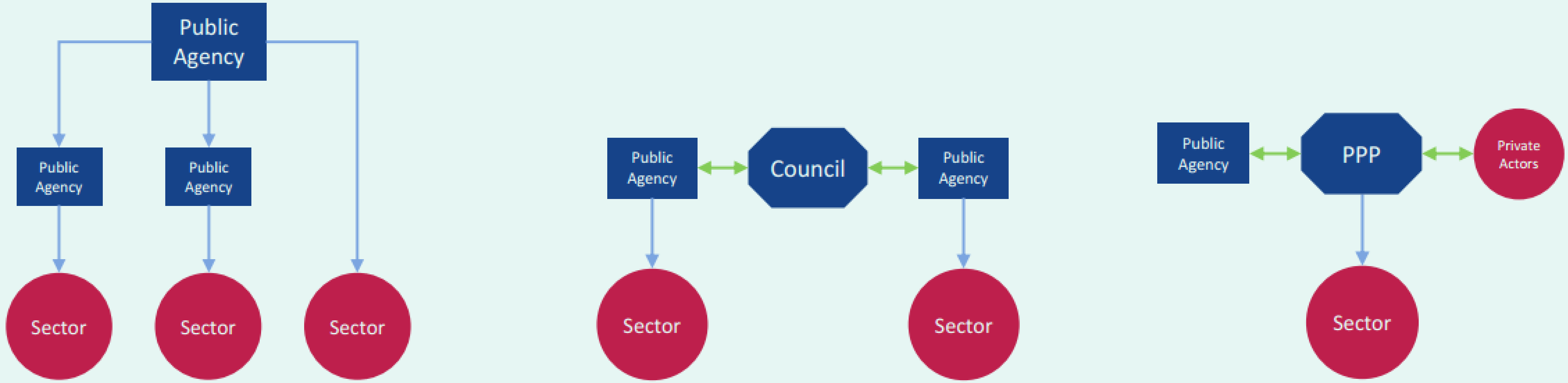
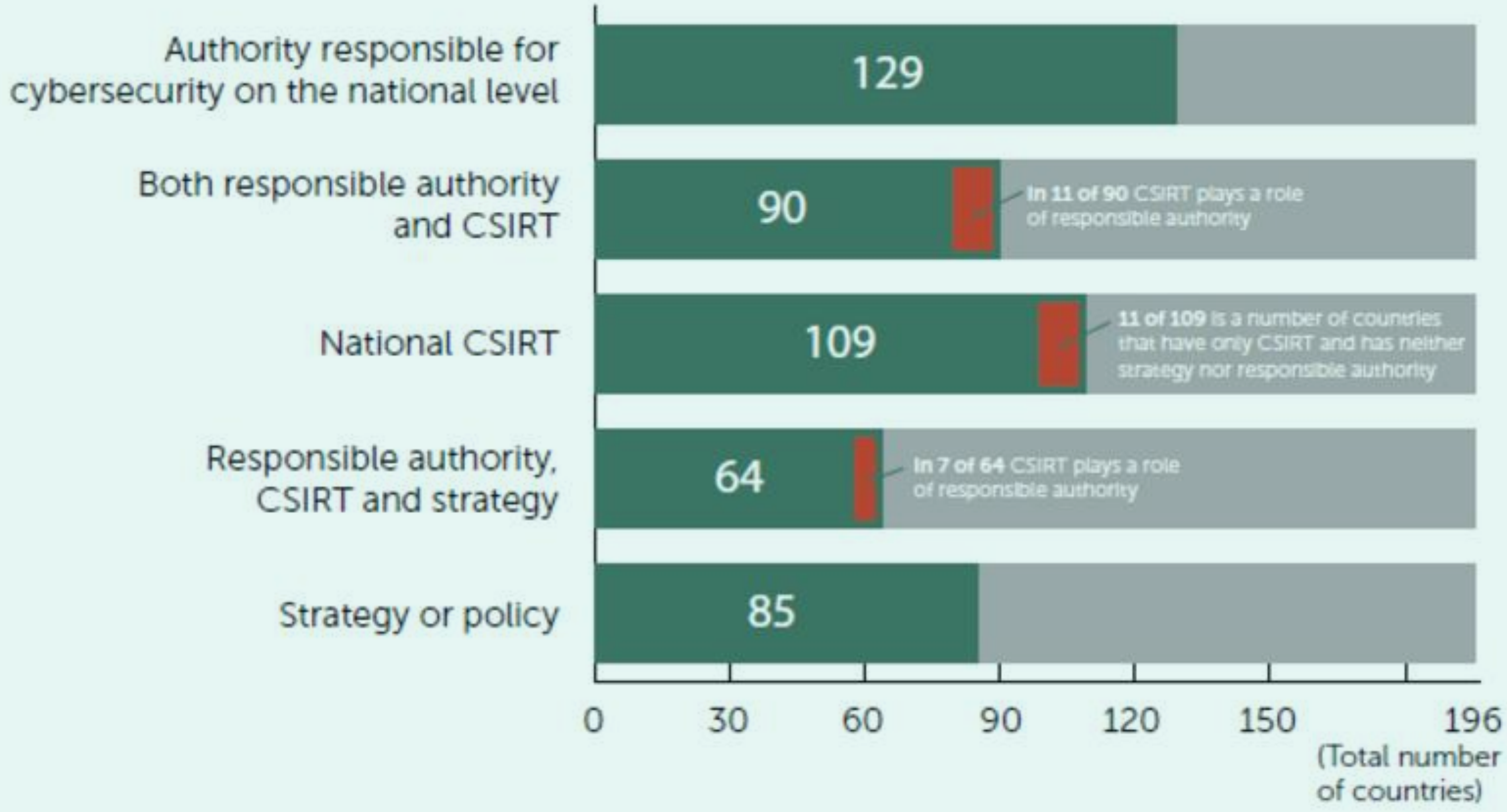


Figure 3-1 – Governance structures

Source: https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport



In 11 of 90 CSIRT plays a role of responsible authority

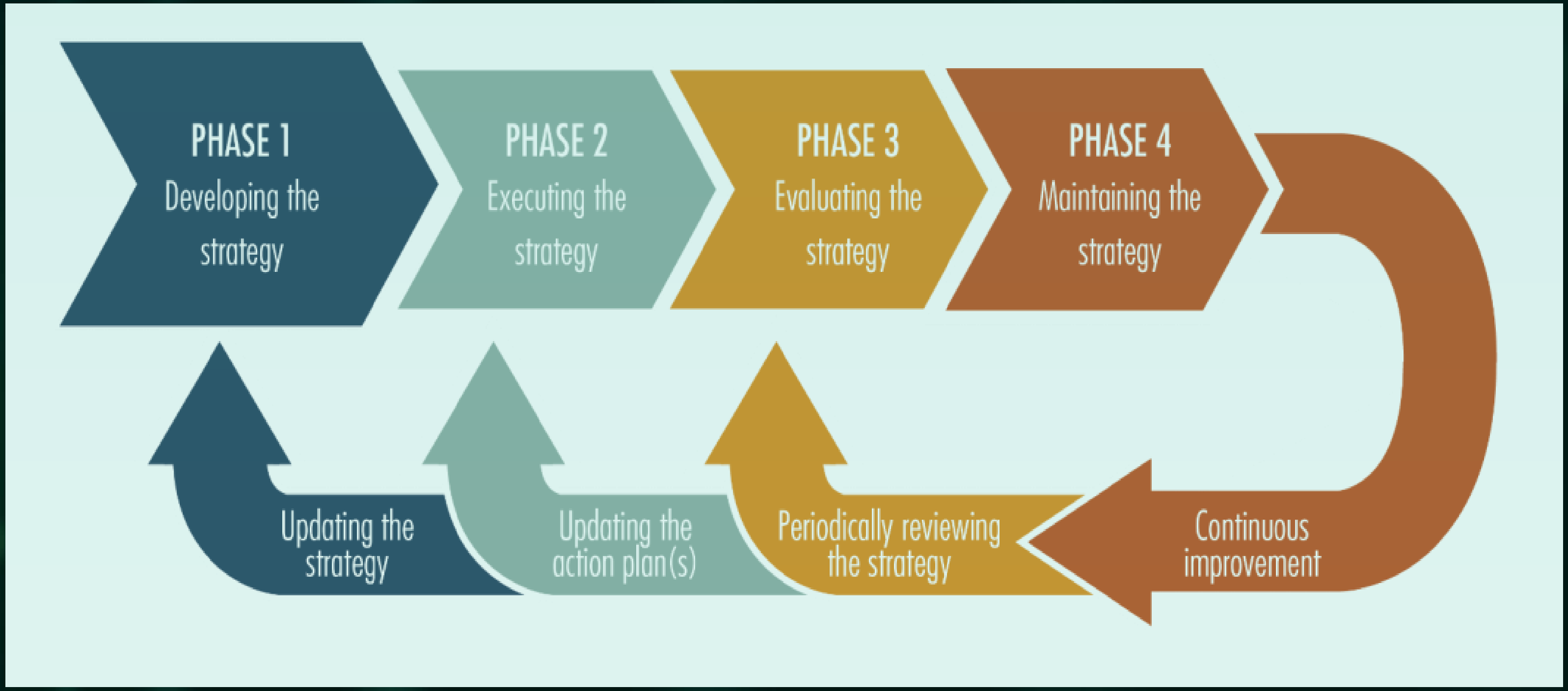
11 of 109 is a number of countries that have only CSIRT and has neither strategy nor responsible authority

In 7 of 64 CSIRT plays a role of responsible authority

Fig. 2. The Global Situation with Main Cybersecurity Governance Indicators

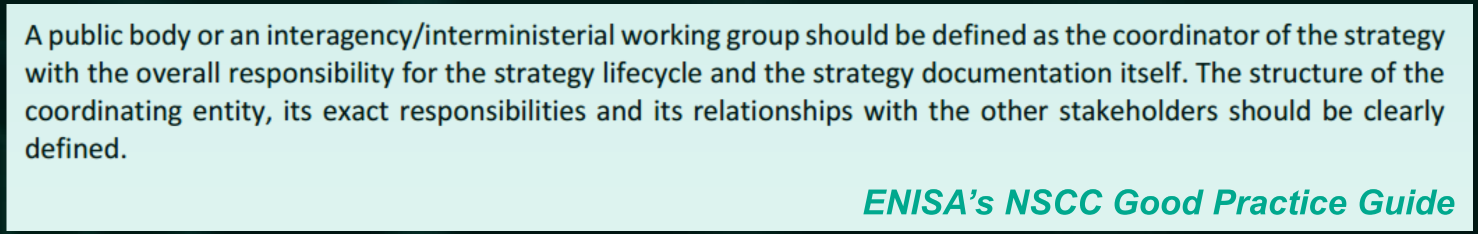
Source: https://ics-cert.kaspersky.com/reports/2016/12/02/critical-infrastructure-protection-governance-around-the-world/

Adaptive Strategies and Frameworks



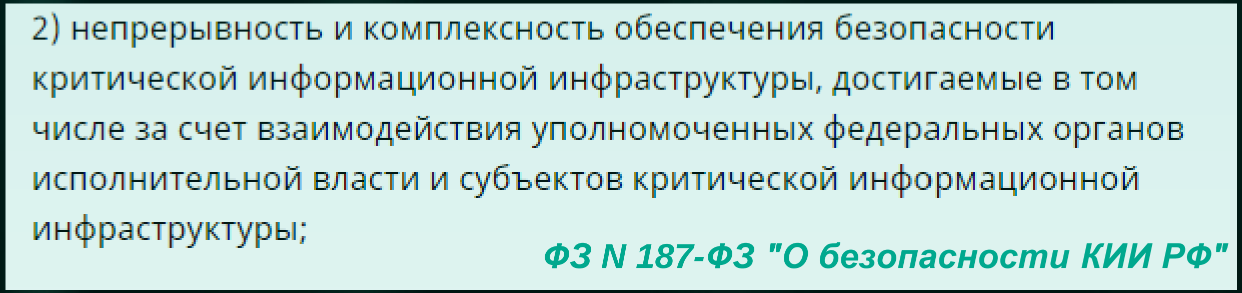
Source: https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport

Structure of responsible authorities



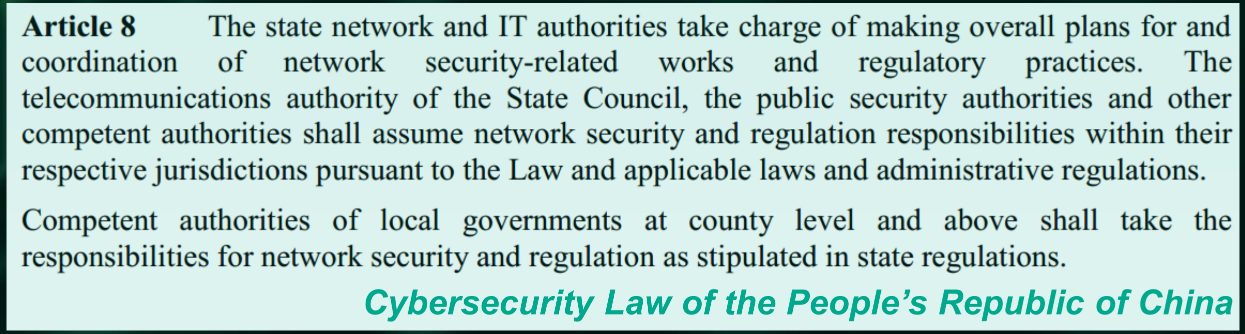
A public body or an interagency/interministerial working group should be defined as the coordinator of the strategy with the overall responsibility for the strategy lifecycle and the strategy documentation itself. The structure of the coordinating entity, its exact responsibilities and its relationships with the other stakeholders should be clearly defined.

ENISA's NSCC Good Practice Guide



2) непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры;

ФЗ N 187-ФЗ "О безопасности КИИ РФ"

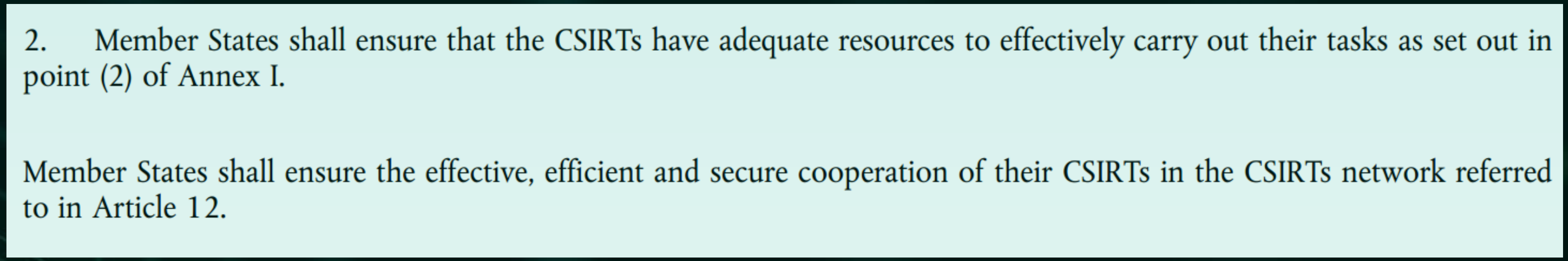


Article 8 The state network and IT authorities take charge of making overall plans for and coordination of network security-related works and regulatory practices. The telecommunications authority of the State Council, the public security authorities and other competent authorities shall assume network security and regulation responsibilities within their respective jurisdictions pursuant to the Law and applicable laws and administrative regulations.

Competent authorities of local governments at county level and above shall take the responsibilities for network security and regulation as stipulated in state regulations.

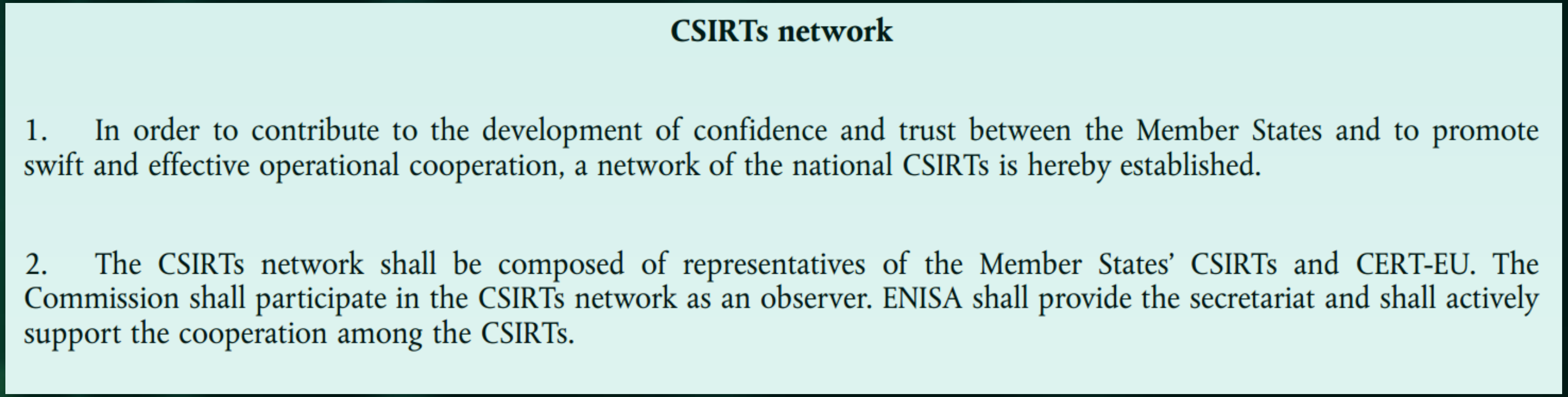
Cybersecurity Law of the People's Republic of China

From the state CSIRT to CSIRT network



2. Member States shall ensure that the CSIRTs have adequate resources to effectively carry out their tasks as set out in point (2) of Annex I.

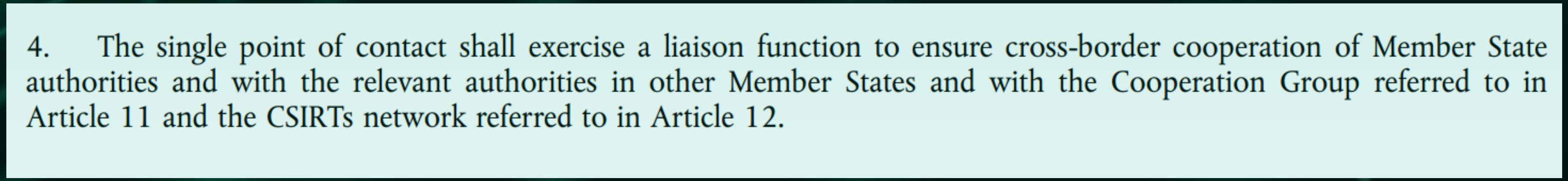
Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network referred to in Article 12.



CSIRTs network

1. In order to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation, a network of the national CSIRTs is hereby established.

2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT-EU. The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support the cooperation among the CSIRTs.



4. The single point of contact shall exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group referred to in Article 11 and the CSIRTs network referred to in Article 12.

PPP evolution

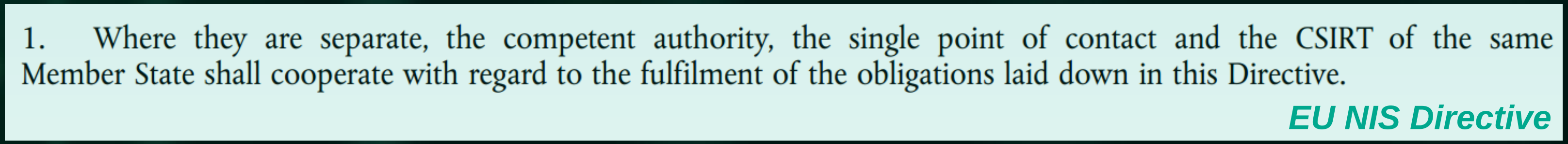
Example: changes in the Dutch National Cyber Security Strategy v2 regarding PPP and related topics

Public-private partnership	Private-public participation
Focus on structures	Focus on networks / strategic coalitions
Formulation of multi-stakeholder model	Clarifying the relationships between the various stakeholders
Capacity-building in the Netherlands	Capacity-building both in the Netherlands and abroad
General approach: deploy wide capacity for resilience-increasing measures	Risk-based approach: balance between protection of interests, threat to interests and acceptable risks in society
Formulation of fundamental principles	Presentation of (policy) vision
From ignorance to awareness	From awareness to capability

Interagency collaboration as key to success

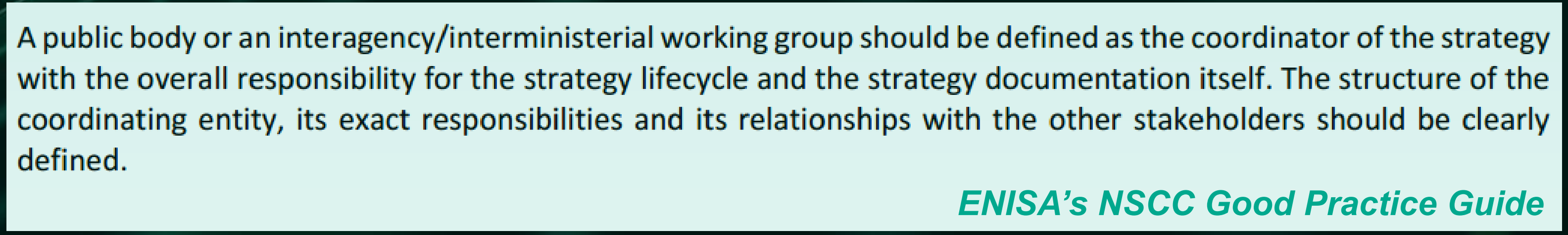
The French ANSSI is an interministerial agency attached to the Prime Minister’s office and acts under the strategic guidance of SGDSN. The agency’s role was strengthened in 2011, when it was declared the national authority for the defence of information systems.

In Austria, the Federal Chancellery of Austria and the Federal Ministry of the Interior share responsibility on a strategic-political level. On an operational level, an “Inner circle” and “Outer circle” form the reliable PPP model.



1. Where they are separate, the competent authority, the single point of contact and the CSIRT of the same Member State shall cooperate with regard to the fulfilment of the obligations laid down in this Directive.

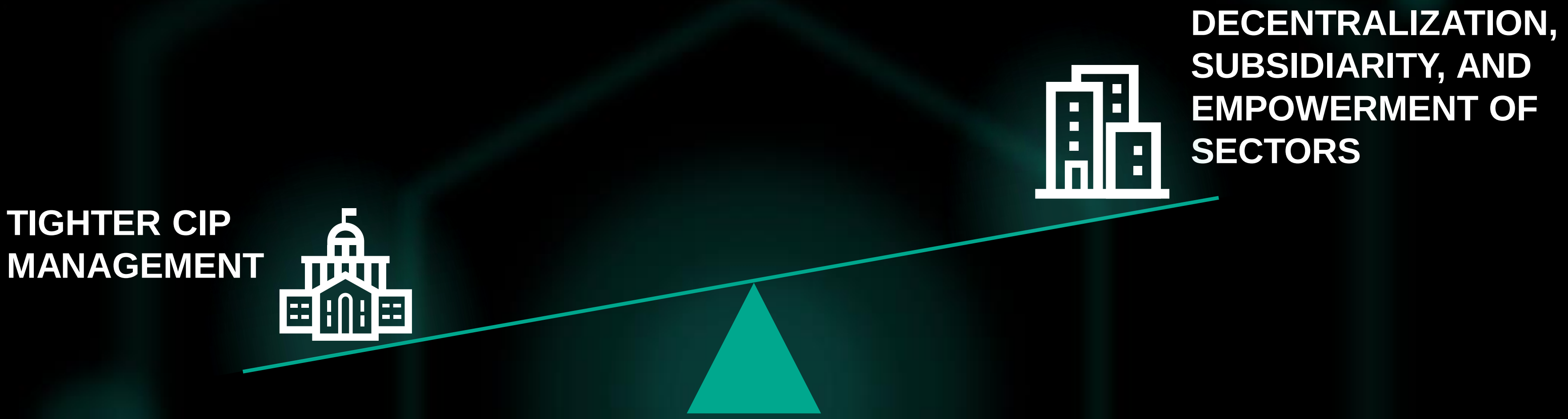
EU NIS Directive



A public body or an interagency/interministerial working group should be defined as the coordinator of the strategy with the overall responsibility for the strategy lifecycle and the strategy documentation itself. The structure of the coordinating entity, its exact responsibilities and its relationships with the other stakeholders should be clearly defined.

ENISA’s NSCC Good Practice Guide

What’s next?



TIGHTER CIP MANAGEMENT

DECENTRALIZATION, SUBSIDIARITY, AND EMPOWERMENT OF SECTORS

How to keep control

Shortened incident response timeframe

Prohibitive fines for violations

Penalty regime for CII stakeholders at all levels etc.

LET’S TALK?

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com

KASPERSKY lab