KU LEUVEN CiTiP

CENTRE FOR IT & IP LAW

CIF – Cybersecurity Initiative Flanders

INFRA STRESS

imec

CIF Lunch Meeting Series Part 1/2

NIS Directive

Stefano Fantin

4.3.2020

Today [1/2]

Background and context (EU cybersecurity policy , basics of EU law)

The NIS Directive

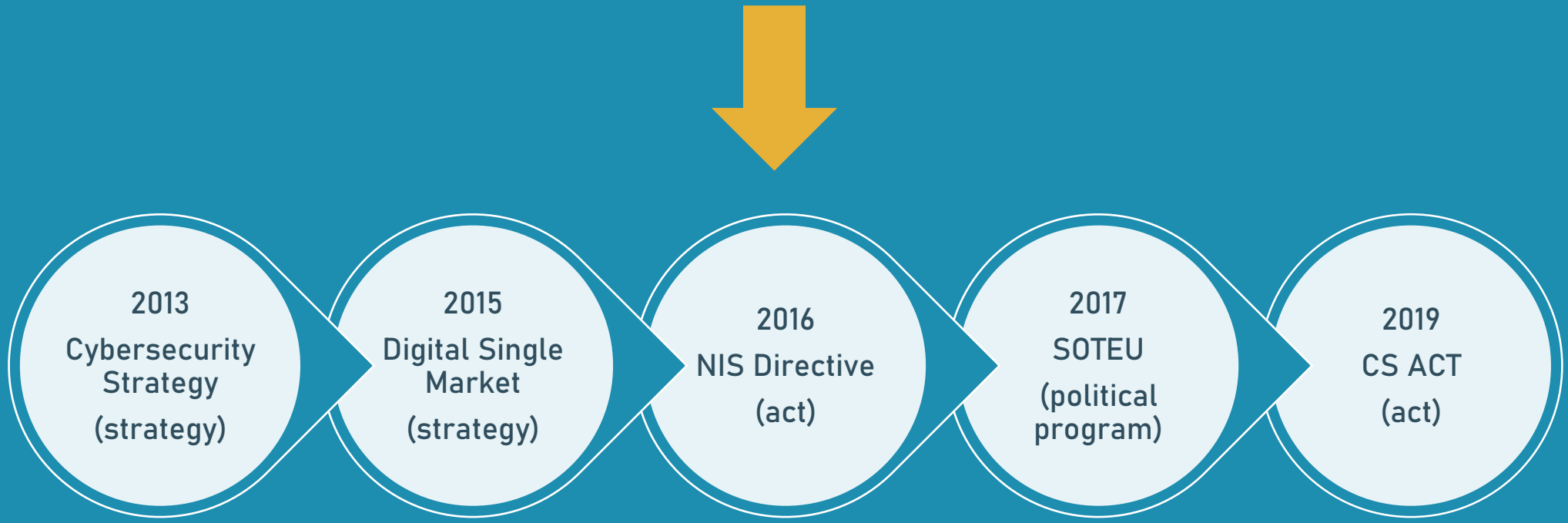
Cooperation and incident handling (Blueprint)

Challenges

Handover to Michiel [part 2/2: Cybersecurity Act]

Background and context: the EU and cybersecurity, a memoir

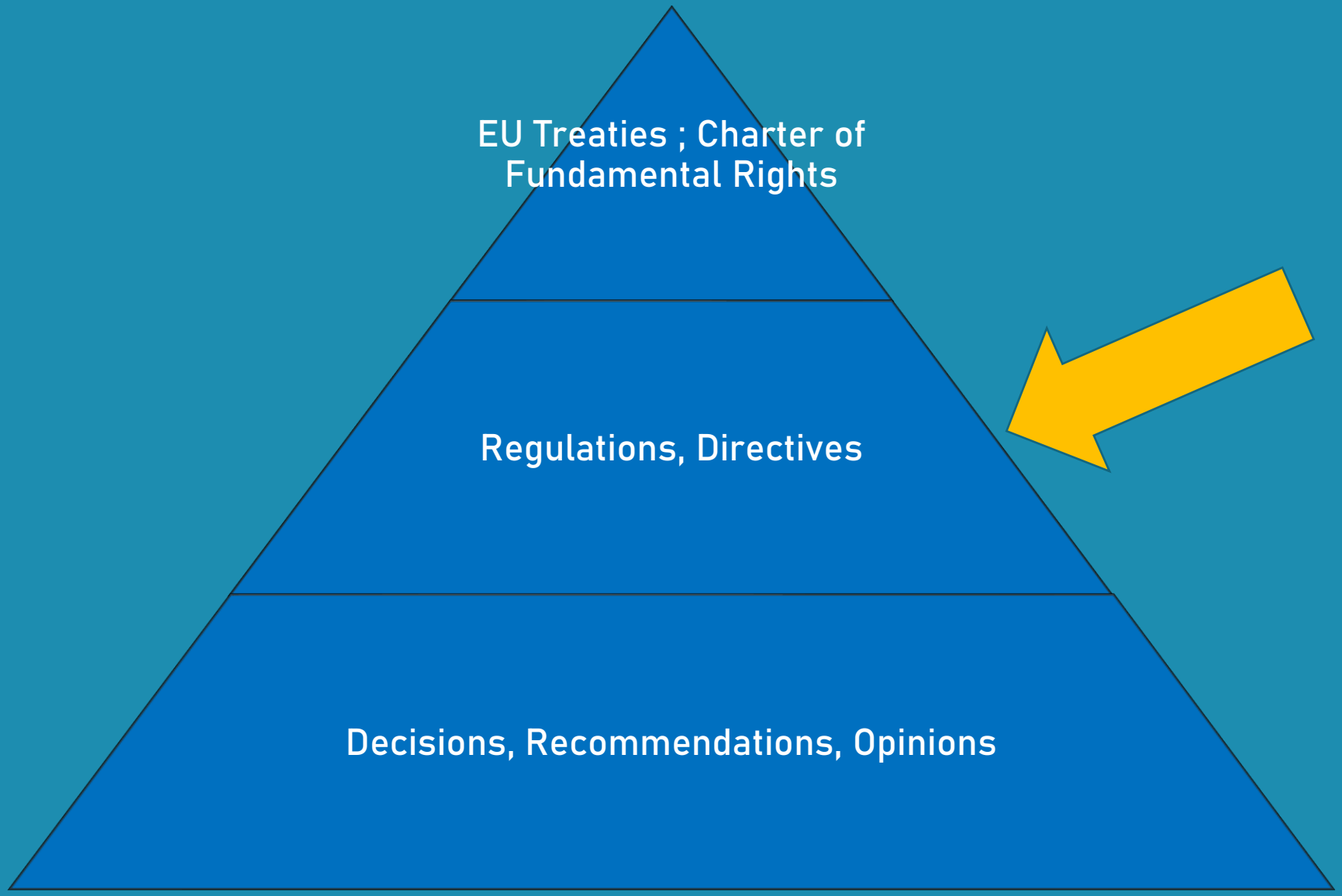
…insufficient level of protection against network and information security incidents, risks and threats across the EU undermining the proper functioning of the Internal market…



Current Initiatives

- NIS Directive
- Blueprint for rapid emergency response
- Cybersecurity Act
- Securing the electoral process
- Cyber defense and cyber diplomacy
- Industrial, Technology and Research Competence Centre
- 5G toolbox

A (rough) EU law hierarchical overview



Regulation vs Directive

	REGULATION Example: cybersecurity Act	DIRECTIVE Example: NIS Directive
EFFECTS	Direct effect	Indirect effect (needs implementation act by national parliament)
ADDRESSEES	Legally binding to the general public or addressed actors	Legally binding to Member States

Competences of the EU

Exclusive	Shared	Supporting
• the customs union • the establishing of the competition rules necessary for the functioning of the internal market • monetary policy for the Member States whose currency is the euro • the conservation of marine biological resources under the common fisheries policy • Common Commercial Policy • conclusion of certain international agreements	• the internal market • social policy, for the aspects defined in this Treaty • economic, social and territorial cohesion • agriculture and fisheries, excluding the conservation of marine biological resources • environment • consumer protection • transport • trans-European networks • energy • the area of freedom, security and justice (Justice and police cooperation) • common safety concerns in public health matters, for the aspects defined in this Treaty • the coordination of economic, employment and social policies • common foreign, security and defense policies (foreign affairs and defense)	• the protection and improvement of human health • industry • culture • tourism • education, youth, sport and vocational training • civil protection (disaster prevention) • administrative cooperation

NATIONAL SECURITY (MS exclusive competence)

Finally, the NIS

*"achieving a **high** common level of security of network and information systems within the Union so as to improve the functioning of the internal market"*

The existing capabilities are not sufficient to ensure a high level of security of network and information systems within the Union.

Rec. 5

Three pillars of the NIS

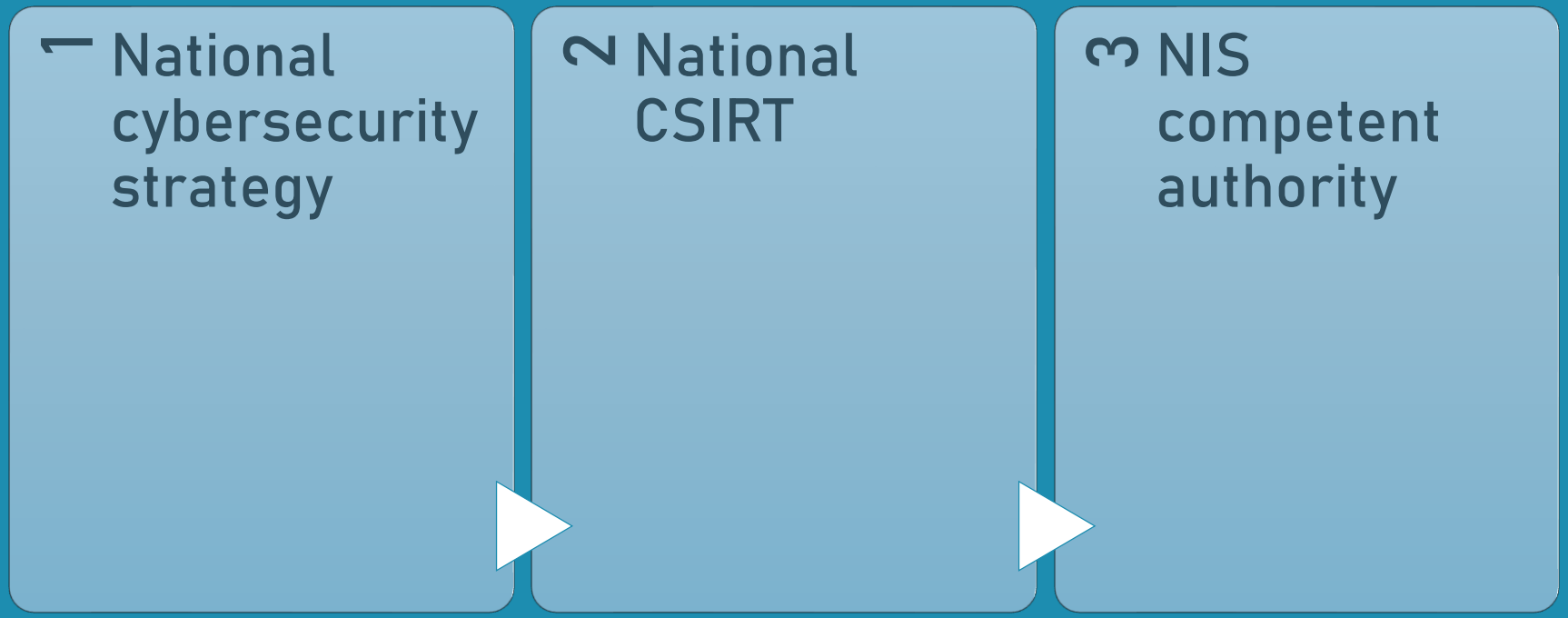
Member States' preparedness

Cross-border cooperation

(security) obligations for specific sectors

1st pillar: Member States' preparedness

i.e., the Directive requires Member States to intervene on their national (vertical) cybersecurity governance:



2nd Pillar: Cross-border cooperation

i.e., establishing national and EU-wide mechanisms for cooperation

1. NIS Cooperation Group
2. National Single Point of Contact (NCG)
3. CSIRT Network

3rd Pillar: obligations for specific sectors

i.e., the Directive asks MSs to impose national obligations

1. Sectors:
   - Operators of essential services;
   - Digital service providers
2. SOTA security requirements
   - Incident notification (business continuity – significant impact)
3. Standardization (‘*light-touch*’)

Results?

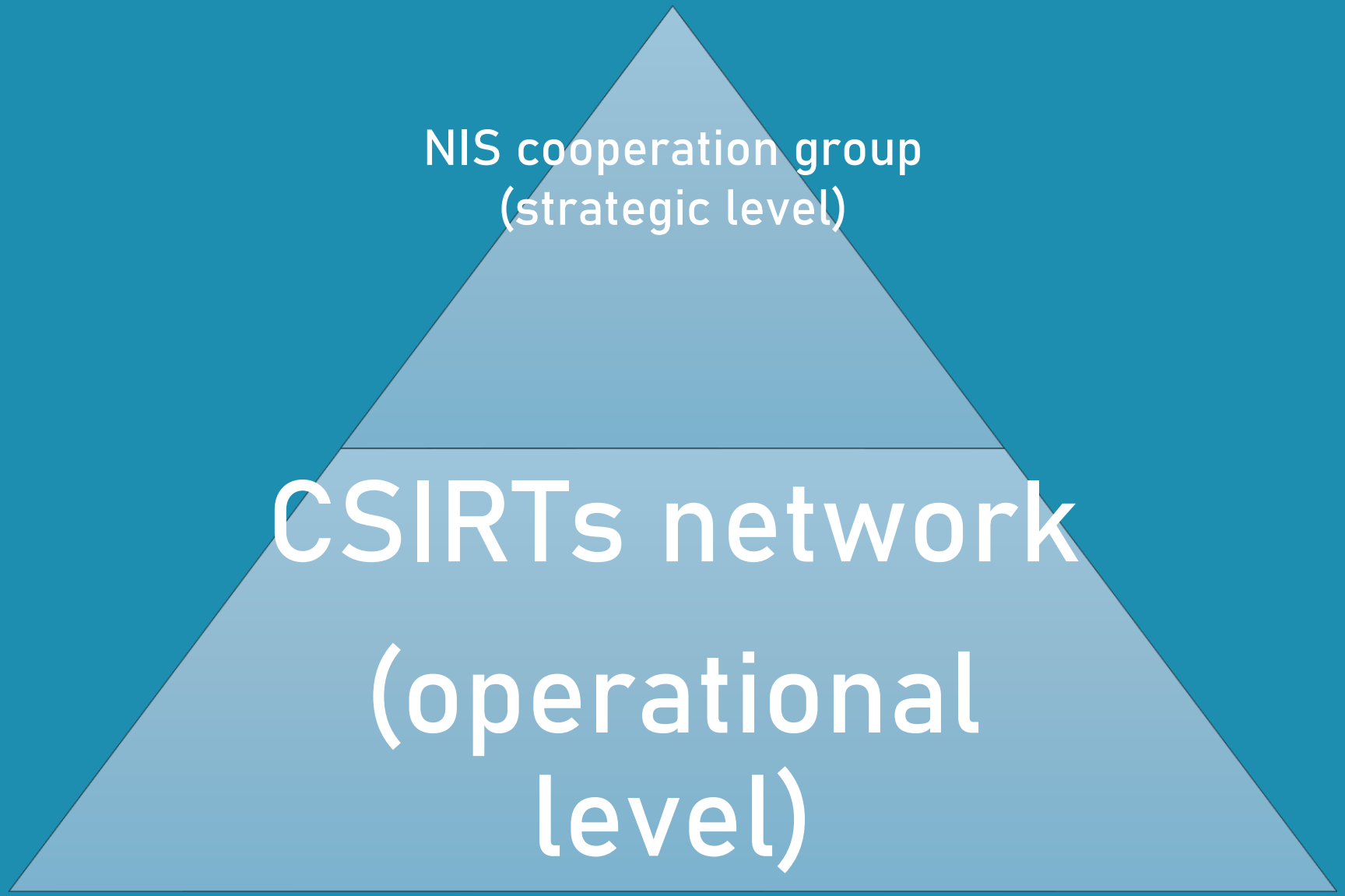
1. Institutionalized cooperation (incl. incident response)

Who receives incident notifications nationally?

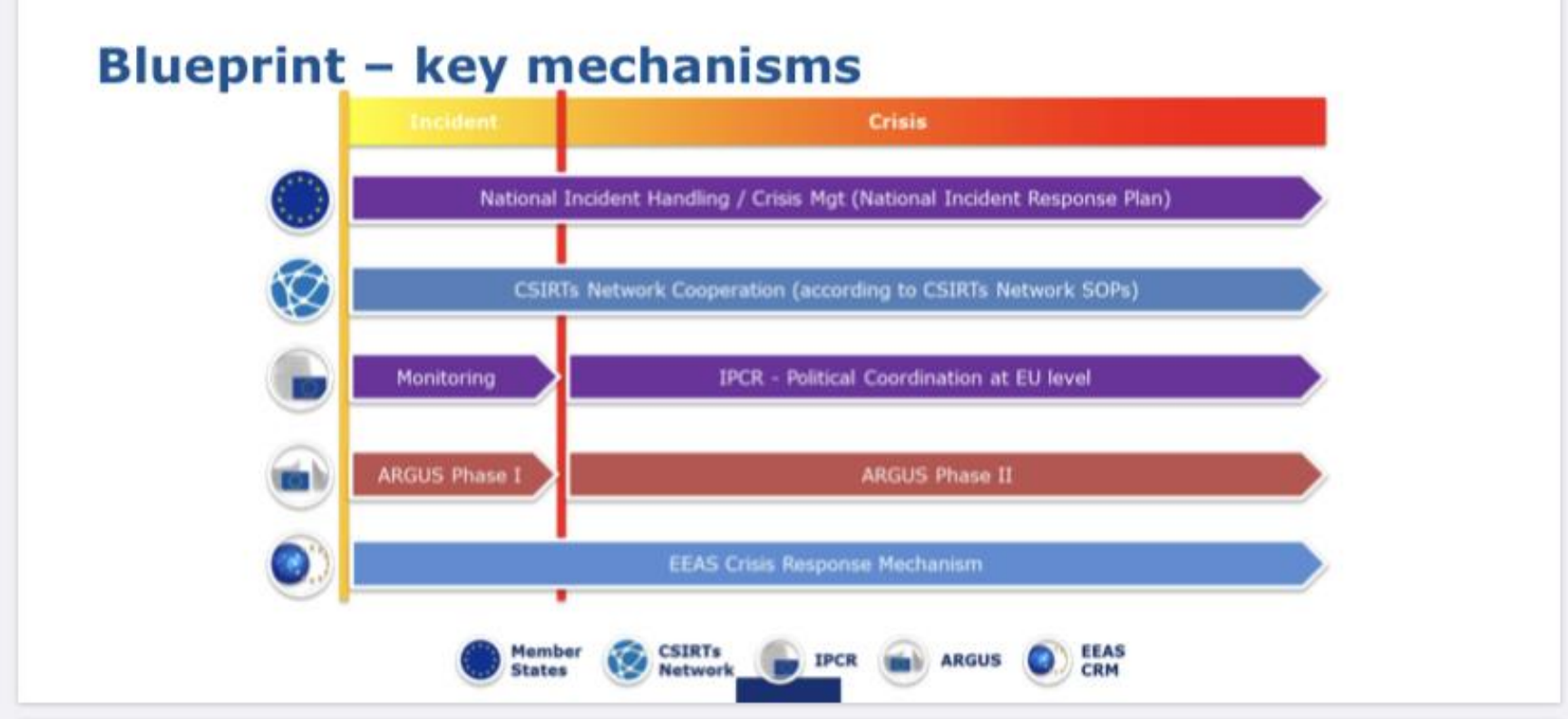
- NIS Competent Authorities or CSIRTs

Who forwards incidents to other countries?

- NIS Competent Authorities or CSIRTs
- SPCs (tasked by NIS CAs or CSIRTs)

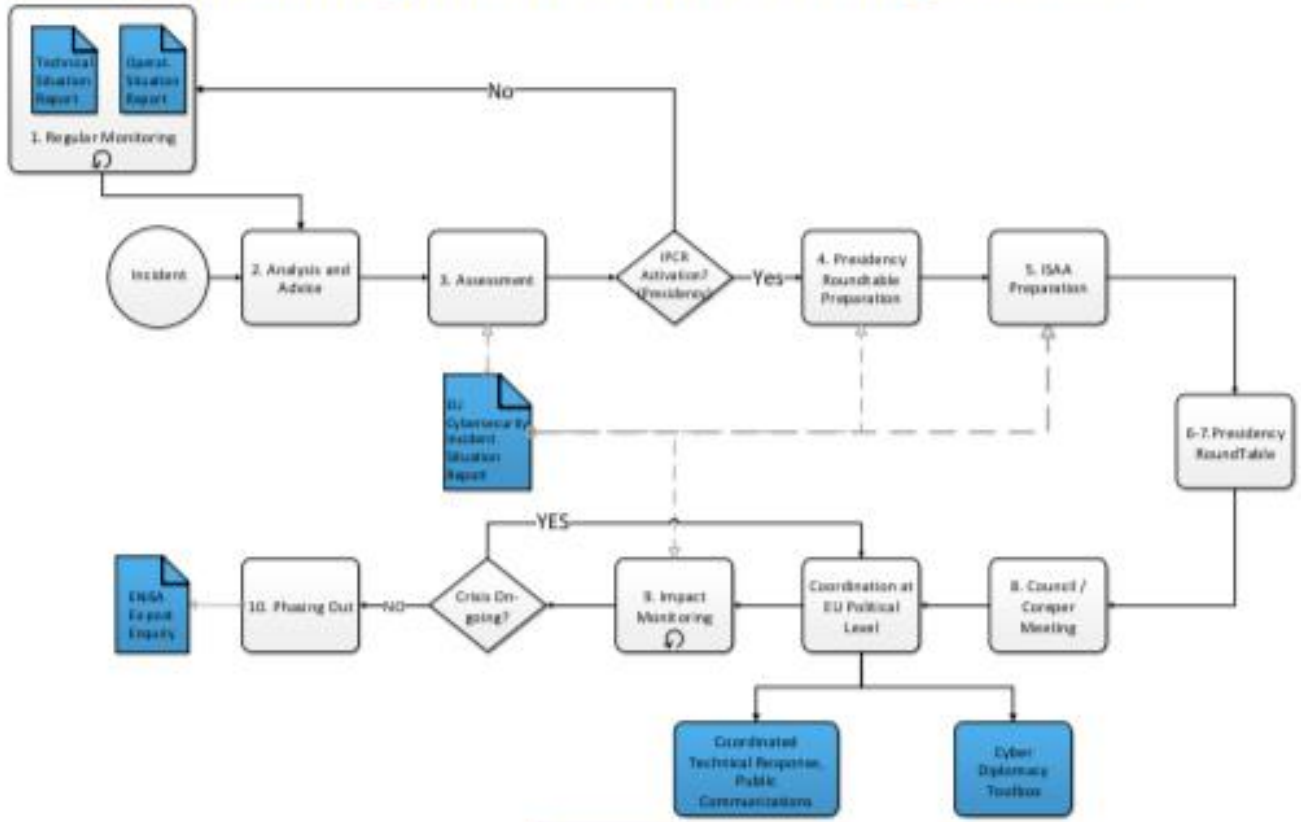


Cross-border large-scale incident response (incl. Blueprint mechanism)



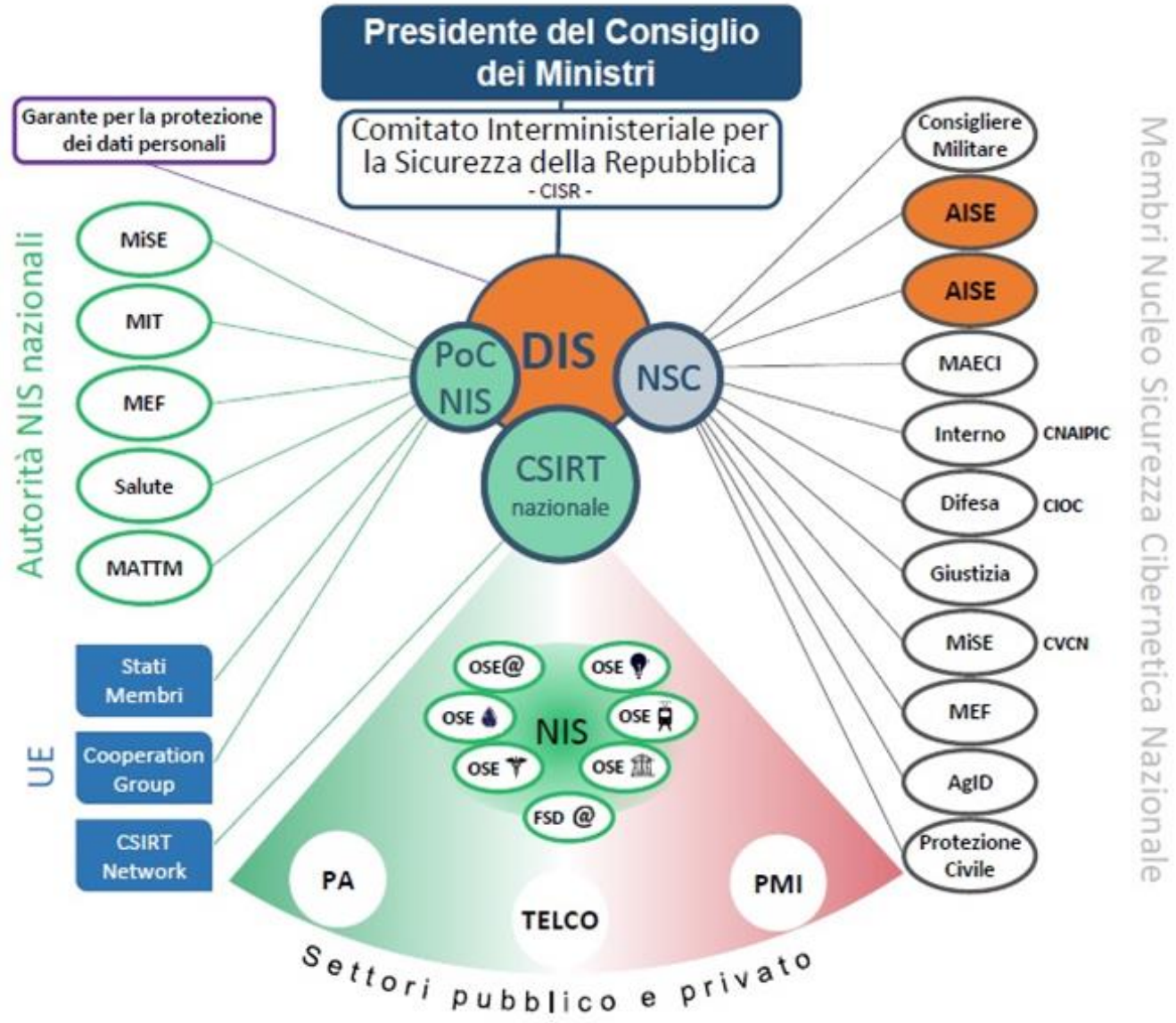
Source: ENISA and European Commission

Recap: Blueprint –integration in IPCR arrangements



Source: ENISA and European Commission

2. National re-arrangement of cybersecurity governance



Source: DIS

Challenges? Yes, many

- Trust private operators – national authorities (economic/financial stakes)
- Trust across Member States (national security stakes)
- Fragmentation of the scope of NIS implementations (reach of EU Directive)
- Confidentiality of national lists of OES/DSPs
- The role of ENISA (not permanent until further legislative initiatives)

THANK YOU

stefano.fantin@kuleuven.be
@s_van_teen

KU Leuven Centre for IT & IP Law (CiTiP) - imec
Sint-Michielsstraat 6, box 3443
BE-3000 Leuven, Belgium

http://www.law.kuleuven.be/citip

KU LEUVEN CiTiP

CENTRE FOR IT & IP LAW

imec

Cybersecurity Act

Michiel Fierens

Agenda

- New role for ENISA
- Pan-European Cybersecurity Certification Scheme
- How will such certification look like in practice?
- Remarks
- Digital Strategy EU

Definition: article 2 (1)

- Cybersecurity means *"the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats"*

ENISA (2004) (Tasks: articles 5-12)

- Permanent mandate <-> temporary
- Operational cooperation and crisis management (Digital Single Market)
- Support to policy implementation and development
- Key role in setting up and maintaining ECCS

European Cybersecurity Certification Schemes

- Increase quality of EU products and services, guarantee their level of cybersecurity
- ICT products, ICT services and ICT processes (broad) (≠ individuals)
- Voluntary: four year probation period
- Union rolling working programme (first one expected 28 June 2020)

Three assurance levels (article 52)

- Basic: minimize known basic risks of incidents and cyberattacks: mostly self-assessment
  - (e.g. no universal default password) (infra ETSI 303 645)

- Substantial: minimize known cybersecurity risks and risk of incidents and cyberattacks carried out by actors with limited skills and resources

- High: minimize risk of SOTA cyberattacks carried out by actors with significant skills and resources

Elements of ECCS (article 54)

- Subject matter and scope (e.g. categories of ICT products/services/processes)
- Purpose
- References to relevant international, European or national standards
- Applicable assurance level(s)
- Self-assessment permitted or not?
- Possible specific requirements for conformity assessment bodies
- Maximum period of validity of certificates issued under ECCS
- ...

How will it look like? (Standards supporting certification, ENISA December 2019)

- ENISA analyzed standards in areas relevant to potential ECCS (IoT, Cloud, E-Health)

- IoT candidate scheme (ETSI 303 645; Eurosmart IoT Certification)
  - Aim of scheme: for most IoT vendors to reach substantial security level through straightforward and non-expensive processes
  - Focus on smart home IoT devices
- Cloud services
  - No self-assessment here!
  - SecNumCloud (ANSSI) & Esquema Nacional de Seguridad (National Security Scheme Spain)

However…

- No clearly defined mechanism for information sharing (recital 54)
- Different national cybersecurity certification authorities
- Third party certification = expensive?
- ECCS <-> liability
- Synergies and trade-offs between certification GDPR and Cybersecurity Act when certifying security of processing operations?

Digital Strategy EU: high-level objectives

- *Fundamental IT security processes are embedded in management practices across the board,*
- *Provision of a cost effective, consistent and balanced infrastructure offer based. At the same time, the resilience of the systems will be raised,*
- *Widening the scope of incident detection and response.*
- *Reinforcing corporate awareness by stepping up the campaign to build awareness.*

Thank you for listening!