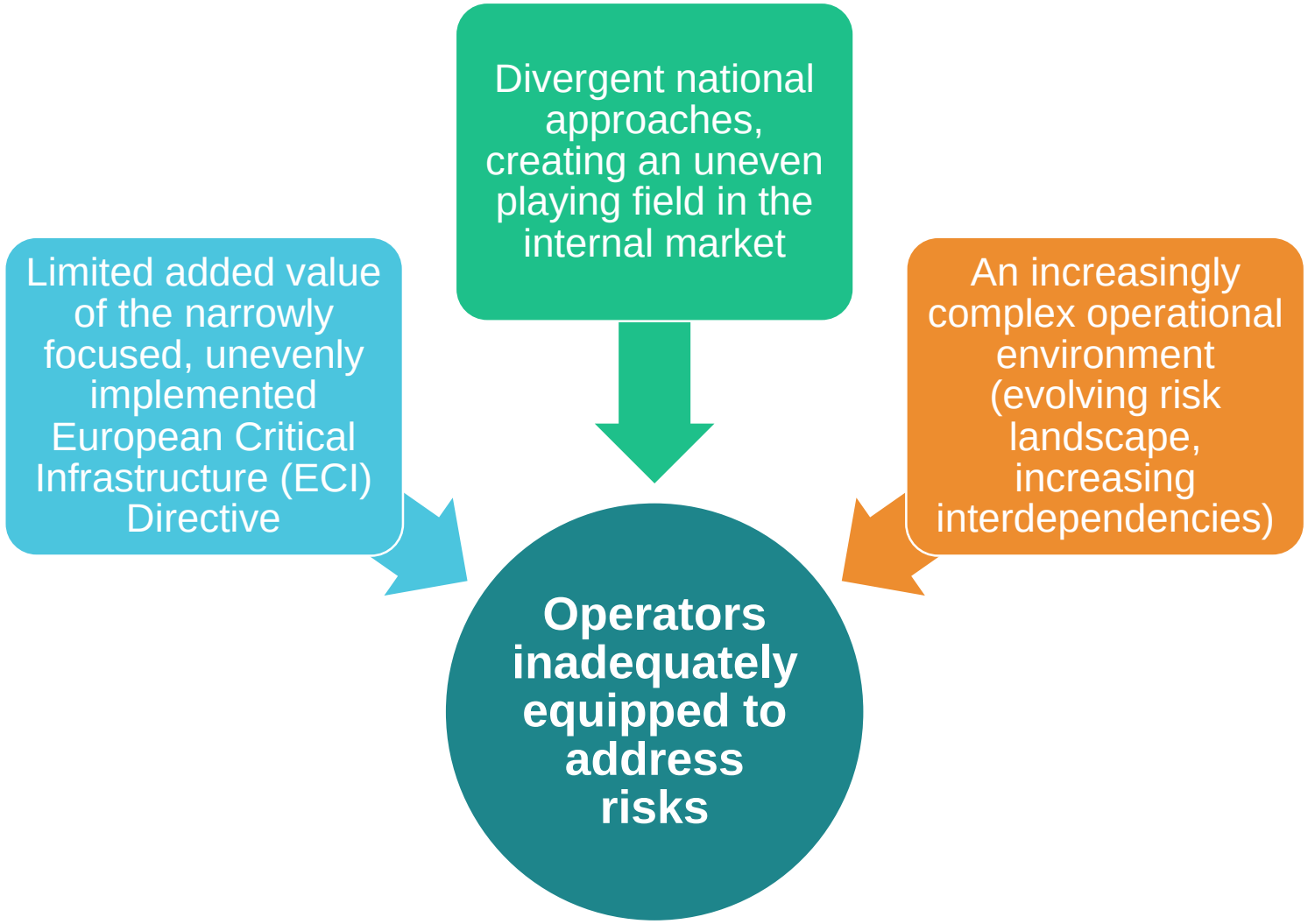
Proposal for a directive on the resilience of critical entities (CER Directive)

European Commission, DG HOME

CIR in the Security Union Strategy

European Commission

A clear need for EU action



Other impetuses

New EU measures, including the NIS Directive and sectoral legislation

A shift in focus (from protection to resilience), while retaining an all-hazards, risk-based approach

Calls for action by the Council, European Parliament, Commission, MS, operators and academia

The main aim of the proposal

- To ensure the provision in the internal market of services that are essential for the maintenance of vital societal functions or economic activities; and
- To enhance the resilience of entities providing such services (‘critical entities’) in the Member States.

What is new in the proposal?

From protection to **resilience**

From the cross-border designation of ECIs to the **identification of critical entities (CEs) at national level**

From 2 to 10 **sectors** (same as in NIS2 annex I)

Risk-based approach at MS and CE level

EU-level support and specific oversight of certain CE (of European significance)

European Commission

Sectoral coverage

- Energy*
- Transport*
- Banking**
- Financial market infrastructures**
- Health
- Drinking water
- Waste water
- Digital infrastructure**
- Public administration
- Space

* Covered by the ECI Directive

** Certain sectoral specificities apply

European Commission

Non-cybersecurity-related risks in focus

- All relevant *non-cybersecurity-related* natural and man-made risks that may affect the provision of essential services, including, for example:
  - Natural disasters
  - Accidents
  - Public health emergencies
  - Antagonistic threats, including terrorist offences.
- *Cybersecurity-related risks* addressed by the NIS2 Directive

Main elements of the proposal

National framework on the resilience of critical entities

- Strategy
- Risk assessment
- Identification of critical entities and entities equivalent to critical entities
- Supervision, enforcement and support

Obligations on critical entities

- Risk assessment
- Resilience measures
- Incident notification

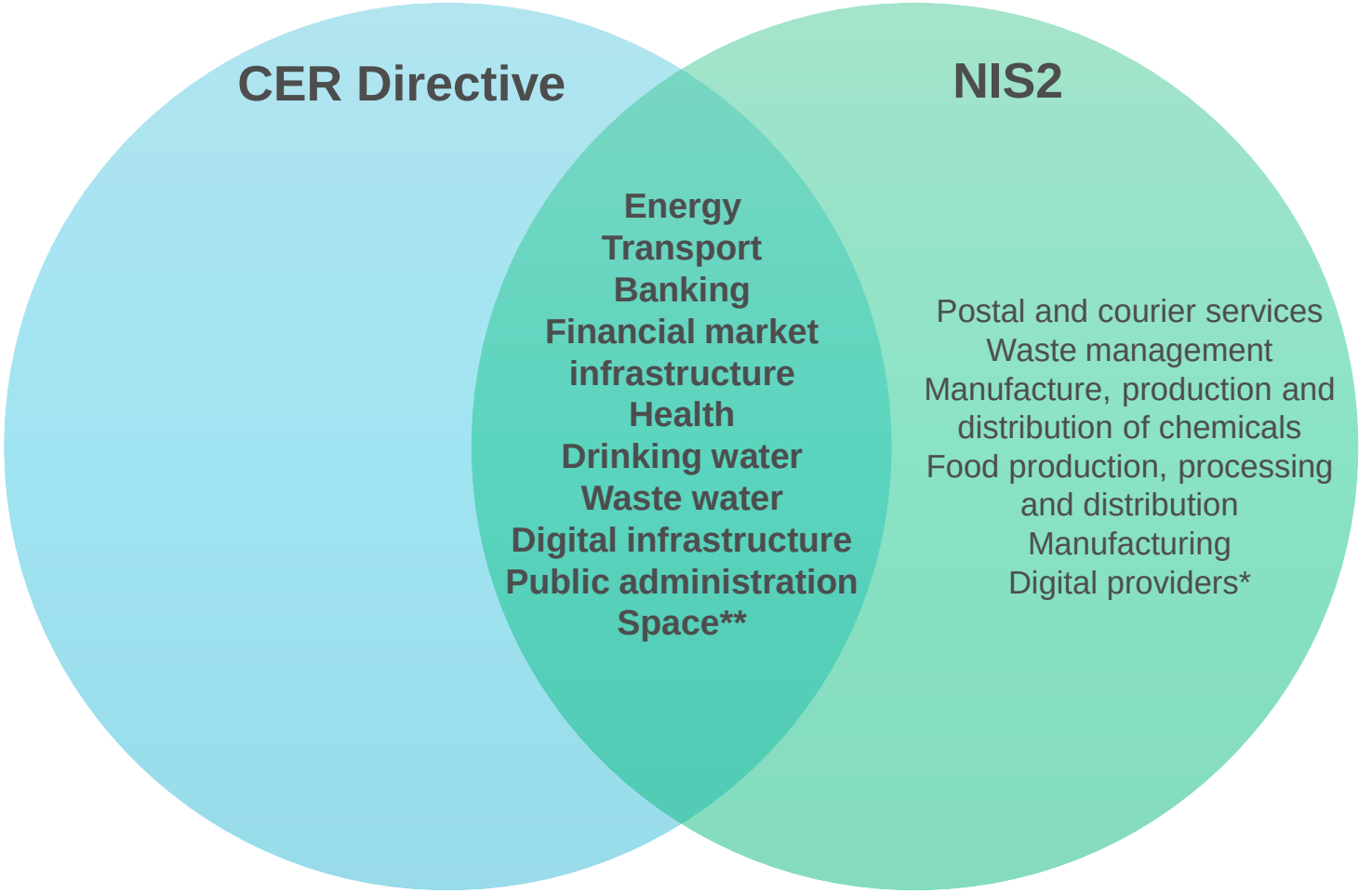
Specific oversight over **critical entities of particular European significance**

Commission support to Member States and critical entities

Strategic cooperation through the Critical Entities Resilience Group

European Commission

The CER-NIS2 interplay



NIS2 is threshold-based, while CER is risk-based

NIS2 seeks to ensure cybersecurity on the part of essential and important entities, while CER ensures the overall (non-cybersecurity-related) resilience of critical entities

CER covers the same ten sectors as the NIS2 'essential entities' list (CER annex = NIS2 annex I)

All critical entities per CER subject to cybersecurity obligations under NIS2

European Commission

* 'Important entities' under NIS2
** 'Essential entities' under NIS2 and 'critical entities' upon identification under the CER Directive

Additional information

https://ec.europa.eu/home-affairs/content/critical-infrastructure-resiliance_en

Contact: HOME-EPCIP@ec.europa.eu

European Commission