A new EU framework to step up the fight against terrorism and boost the EU's resilience

European Commission/ DG Home/
Counter Terrorism Unit

Marc Léoutre

March 30, 2021

EU Counter Terrorism agenda

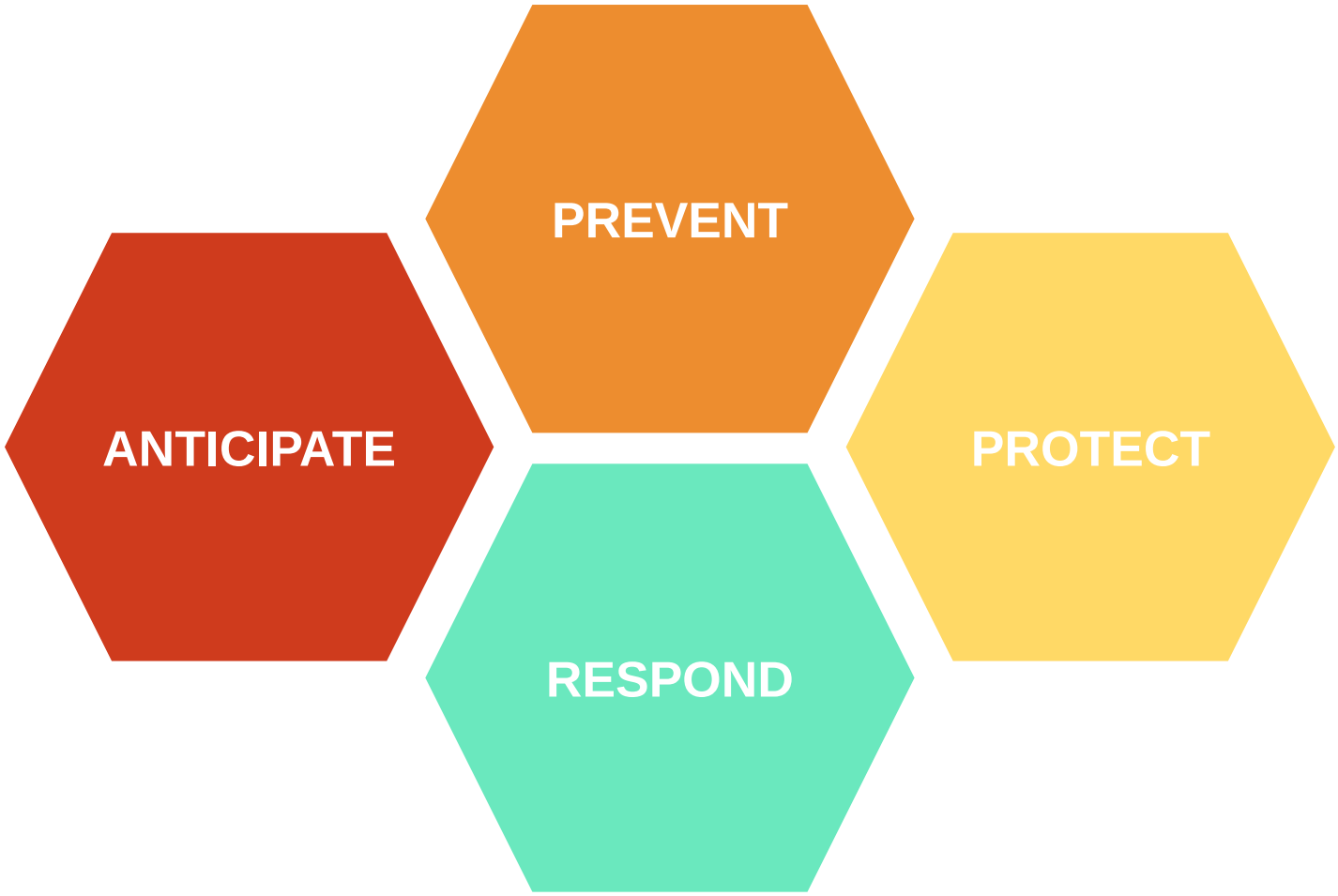
A strategic roadmap to support Member States in better anticipating, preventing, protecting and responding to the terrorist threat.

European Commission

CT agenda for the EU

- EU Security Union Strategy 2020-2025
- A counter-terrorism strategy for the coming years
- Adoption 09.12.2020
- Combination of implementation of existing instruments, finalisation of instruments under development, and new proposals

Main components



European Commission

Anticipate

Anticipating blind spots and staying ahead of the curve

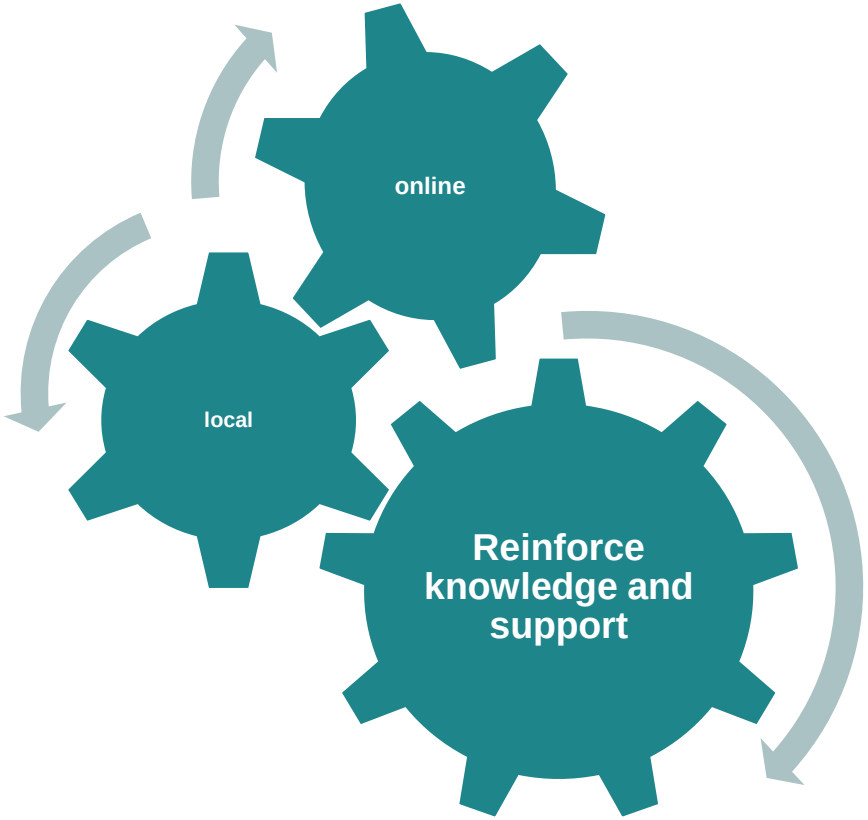
- Integrating strategic intelligence in counter-terrorism policies
- EU Protective Security Advisory missions
- Artificial Intelligence
- Detection
- Drones

European Commission

Prevent

Preventing radicalisation leading to violent extremism

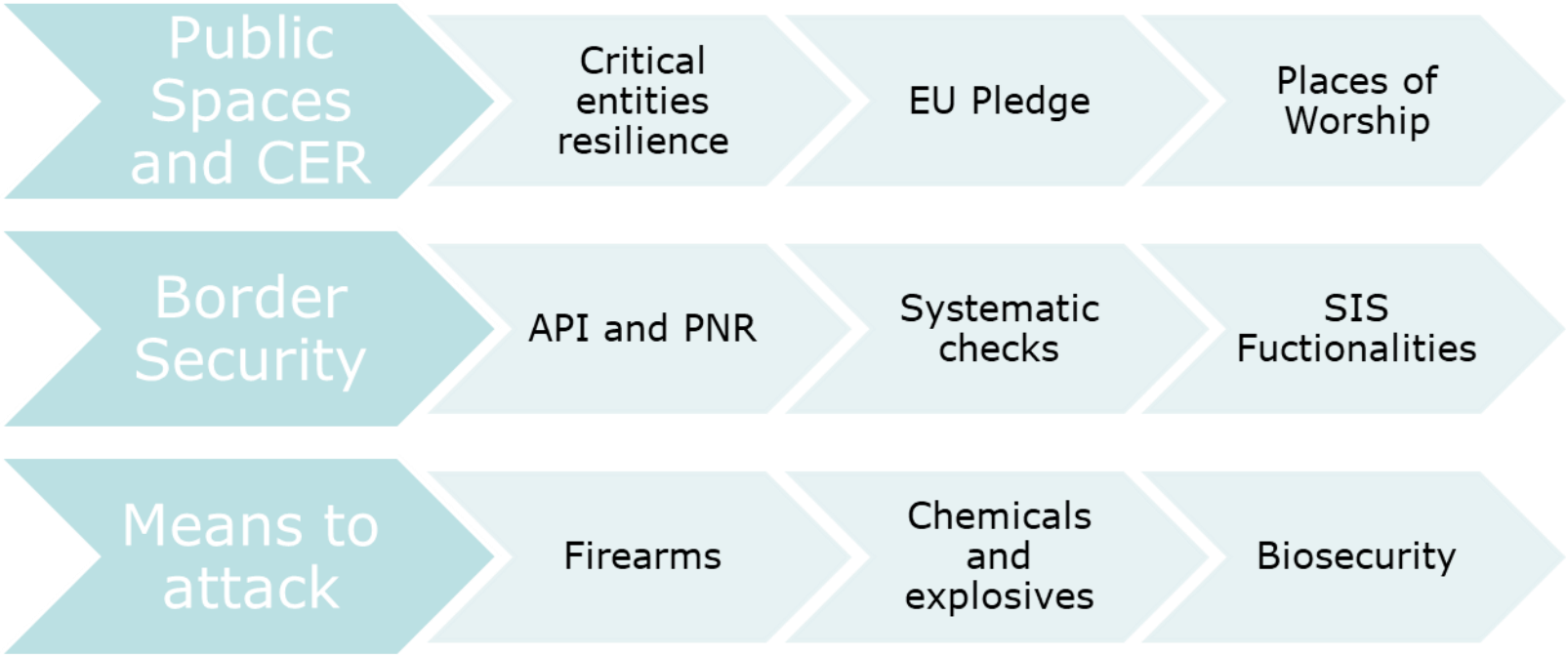
- Countering extremist ideologies online
- Local dimension
- Prison/rehabilitation
- Ideologies



European Commission

Protect

Reducing vulnerabilities to better protect against potential attacks



European Commission

Respond

Swift and decisive actions after an attack

- Strengthening Europol
- EU police cooperation code
- Revision Prüm
- Digital evidence and encryption
- Victims' rights

European Commission

International cooperation

External CT engagement

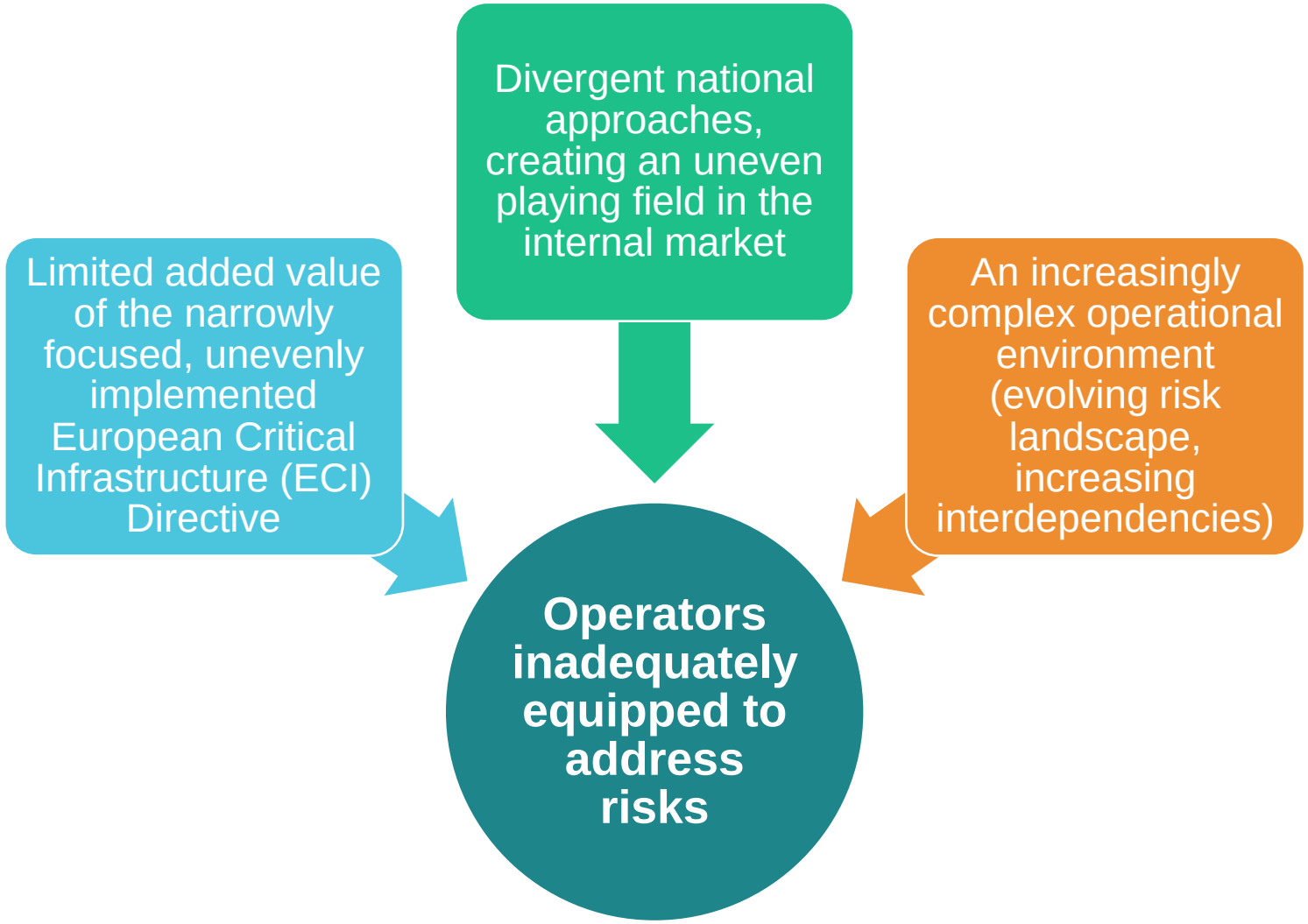
- Cooperation with Western Balkans partners
- Strengthening cooperation with priority countries in the Southern Neighbourhood
- International and regional organisations

Commission proposal for a directive on the resilience of critical entities

To enhance the resilience of critical entities providing essential services in the EU

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 proposal’s main aim

To ensure the provision in the internal market of services essential for the maintenance of vital societal functions or economic activities by enhancing the resilience of entities providing such services (‘critical entities’) in the Member States.

The proposal – what‘s new?

Protection
=>
resilience

Cross-border designation of European critical infrastructures => **identification of critical entities at national level**

2 sectors =>
10 sectors
same as in annex I of NIS2 proposal

Risk-based approach:
at level of Member States and at level of critical entities

EU level support & specific oversight
of entities of European significance

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

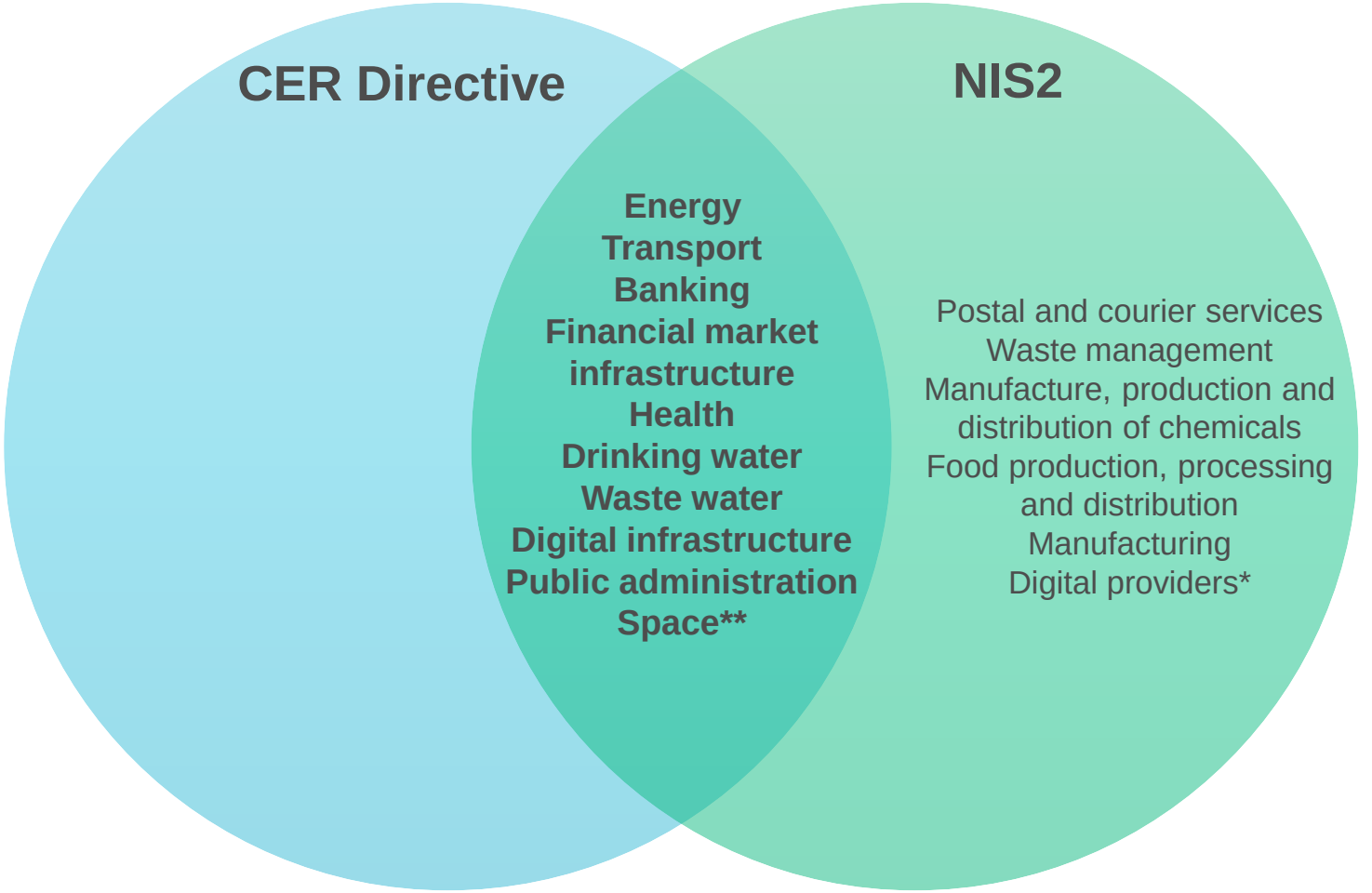
Specific oversight over **critical entities of particular European significance**

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 Directive ensures the overall (non-cybersecurity-related) resilience of critical entities
- The CER Directive covers the same ten sectors as the NIS2 ‘essential entities’ list: CER Directive annex = NIS2 Directive annex I
- All critical entities identified under CER Directive are subject to cybersecurity obligations under NIS2

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

European Commission

On the transport sector specifically

Sub-sector	Type of entity
Air	- Air carriers - Airport managing bodies - Traffic management control operators providing ATC services
Rail	- Infrastructure managers - Railway undertakings
Water	- Inland, se and coastal passenger and freight water transport companies - Managing bodies of ports - Operators of vessel traffic services
Road	- Road authorities - Operators of Intelligent Transport Systems

Link to the annex to the proposal available on DG HOME's website: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/15122020_proposal_directive_resilience_critical_entities_annex-1_com-2020-829-1_en.pdf

European Commission

Marc Léoutre
Policy officer

European Commission
Directorate-General for Migration and Home Affairs (DG HOME)
Counter-Terrorism Unit (D2)
E-mail: marc.leoutre@ec.europa.eu
Phone : +32 2 29 81189
@EUHomeAffairs