ITU Events

ITU Regional Cybersecurity Forum for Europe and CIS

27–28 February 2020
Sofia, Bulgaria

Follow us on twitter: @ITU_EUR & @ITUMoscow
www.itu.int/go/EURCIS_CSForum20

ITU Regional Initiative for Europe on enhancing trust and confidence in the use of ICTs

ITU Regional Initiative for CIS on the development and regulation of infocommunication infrastructure to make cities and human settlements inclusive, safe, and resilient

Hosted and co-organized by:

REPUBLIC OF BULGARIA
Ministry of Transport, Information Technology and Communications

REPUBLIC OF BULGARIA
State e-Government Agency

ITU

5G security initiatives

Visiola Pula

Sofia, 27 Feb. 2020

Outline

EU Cybersecurity regulatory landscape
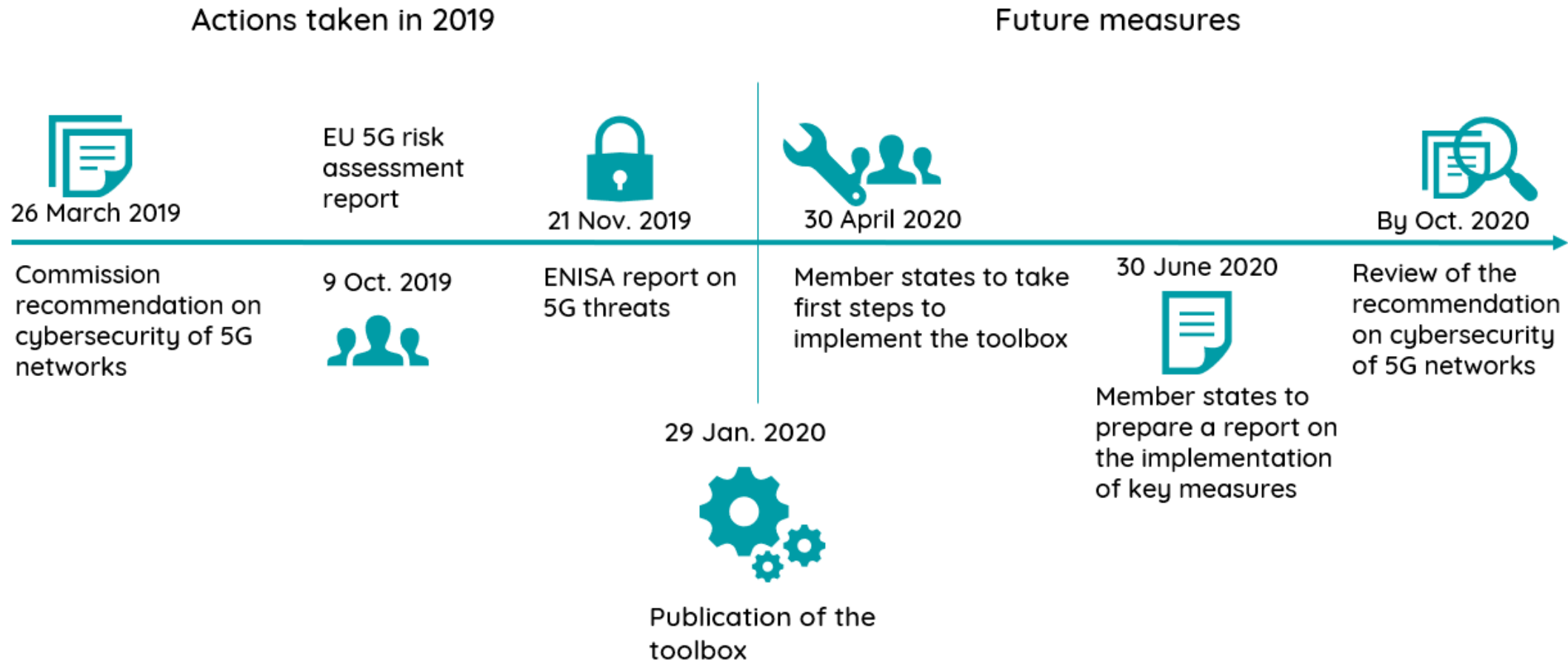
National 5G security initiatives
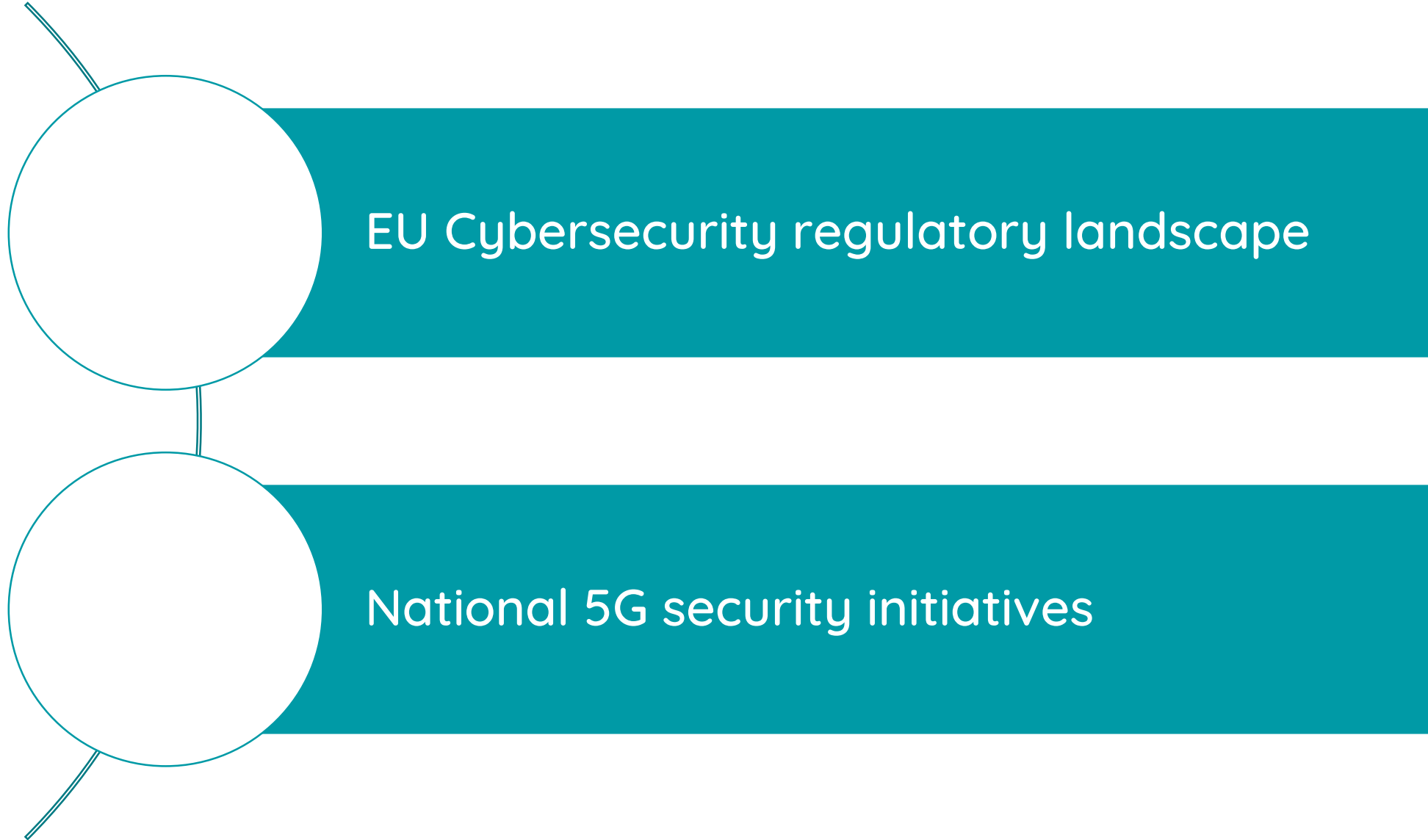
EU cybersecurity regulation

EU cybersecurity framework in a nutshell

Instrument	Content
Telecoms framework (incl. e-Privacy Directive)	• Security measures • Security and data breach reporting requirements for providers of electronic communications services (ECS) and networks
Directive on the security of networks and information systems (NIS)	• Security measures • Security incident reporting requirements for operators of essential services (OES) and digital services providers (DSP)
EU Cybersecurity Act	Framework for voluntary EU cybersecurity certification of ICT products, services and processes
5G Cybersecurity Recommendation	European Commission's 5G security recommendations for EU member states
EU 5G toolbox	Lists measures (strategic and technical) to mitigate security threats associated with 5G networks

EU 5G security timeline

Actions taken in 2019

Future measures

26 March 2019

Commission recommendation on cybersecurity of 5G networks

9 Oct. 2019

EU 5G risk assessment report

21 Nov. 2019

ENISA report on 5G threats

29 Jan. 2020

Publication of the toolbox

30 April 2020

Member states to take first steps to implement the toolbox

30 June 2020

Member states to prepare a report on the implementation of key measures

By Oct. 2020

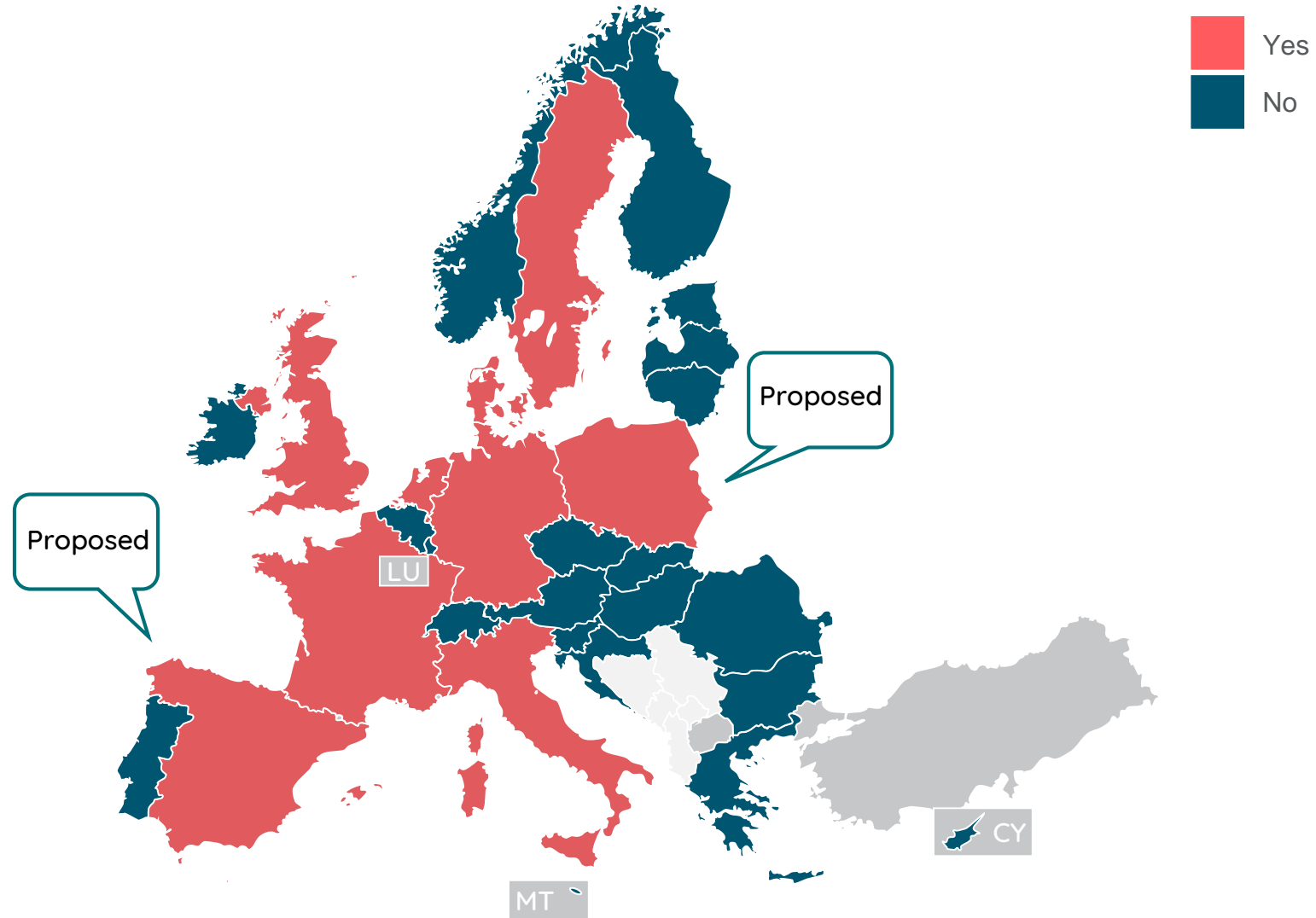Review of the recommendation on cybersecurity of 5G networks

CULLEN
INTERNATIONAL

A candidate security certification scheme for 5G?
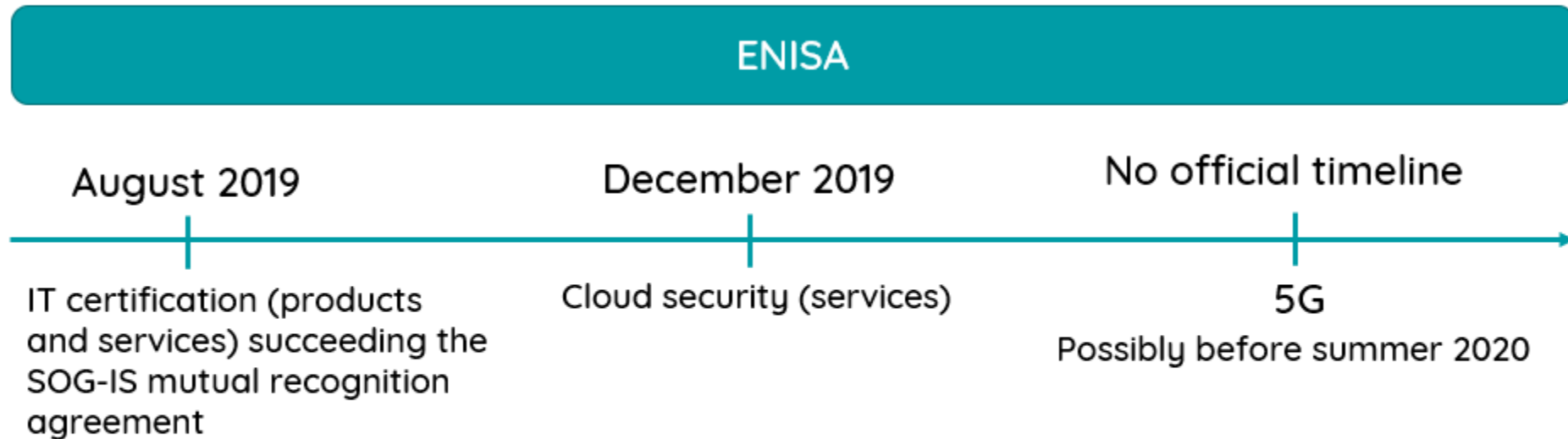
ENISA

August 2019

IT certification (products and services) succeeding the SOG-IS mutual recognition agreement

December 2019

Cloud security (services)

No official timeline

5G
Possibly before summer 2020

CULLEN
INTERNATIONAL

National 5G security initiatives

Common features in 5G security initiatives

Measures	Countries
Direct ban	US 🇺🇸
Possibility to ban equipment from certain suppliers	NL 🇳🇱 SE 🇸🇪 UK 🇬🇧
Authorisation to acquire/use certain equipment	FR 🇫🇷 IT 🇮🇹
Based on general telecoms regulation	DE 🇩🇪 DK 🇩🇰

CULLEN
INTERNATIONAL

Law protecting defence in 5G (Aug. 2019)

Telecoms operators → Certain equipment (decree) → PM prior authorisation
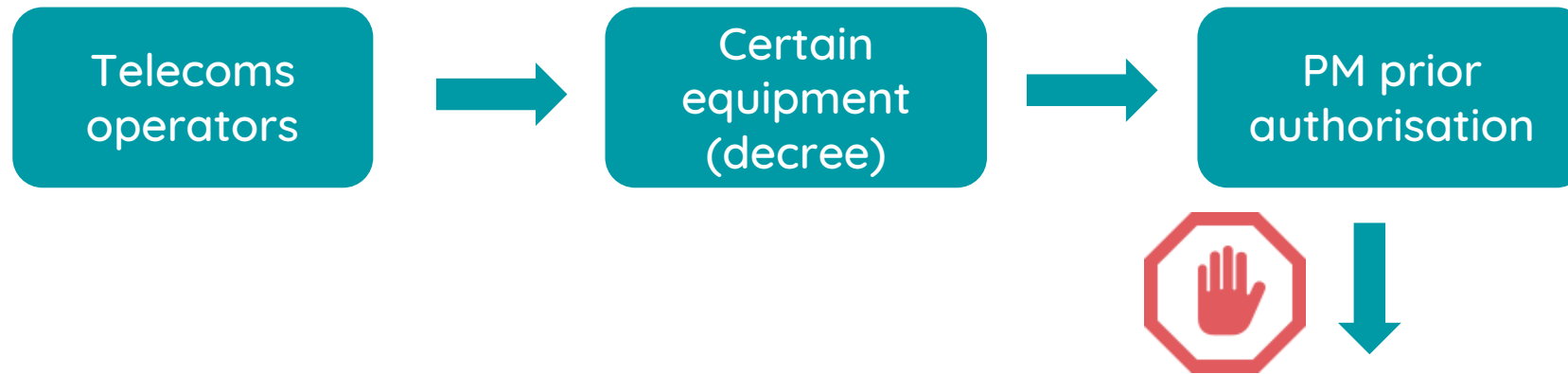
Serious risk to defence and national security interests

No response within two months

CULLEN INTERNATIONAL

Law addressing security of 5G

Key provisions

Notification obligation → Operators → Contracts concluded for the supply of ICT tools (5G) with companies **outside of Europe** to notify it to the National Centre of Assessment and Notifications (NCAN) → NCAN has 45 days to decide if imposing tests

Gov. veto power → On ICT tools used in 5G when supplied by companies **outside Europe**. To be notified to the gov. 10 days in advance

Golden share → Block foreign acquisition giving the buyer control of a company (assets) belonging to a strategic sector
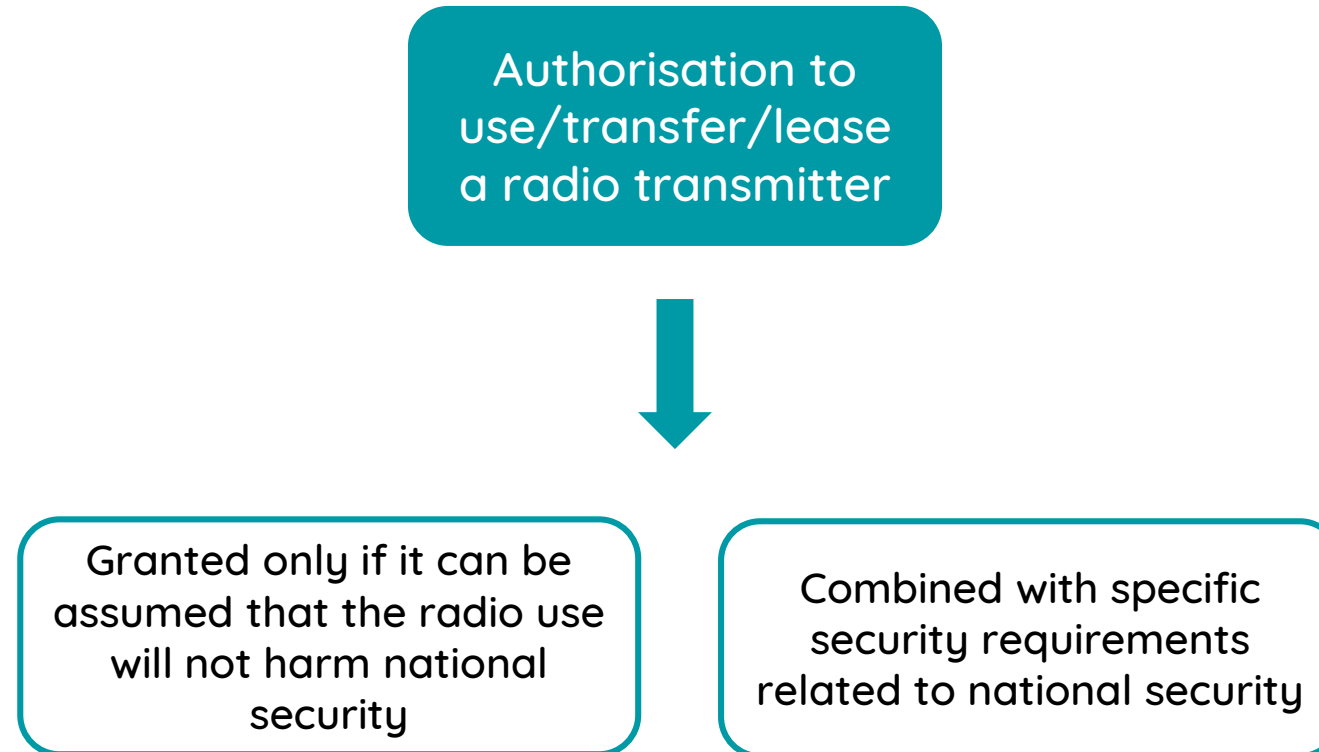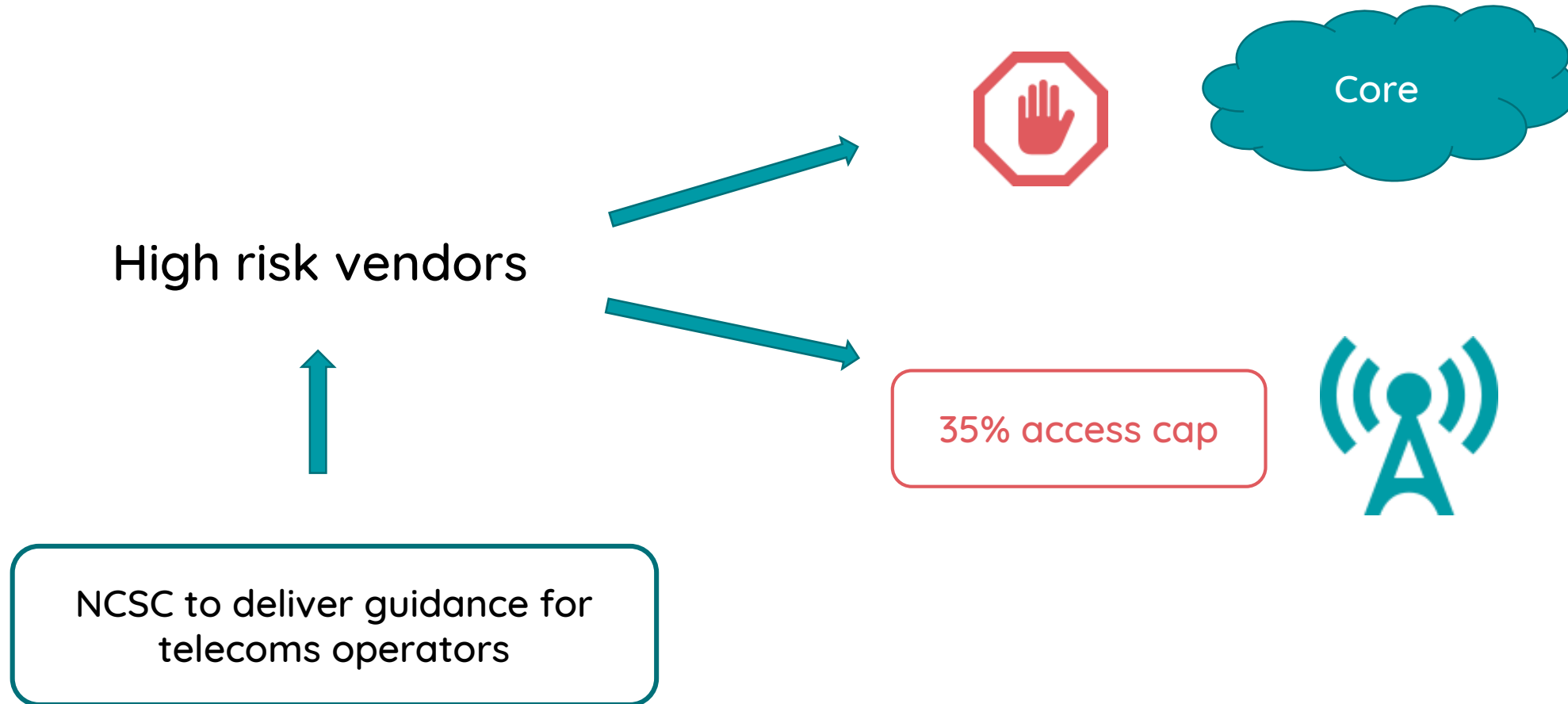
Outside Europe

- Does not have a permanent establishment or principal place of business within the EU
- Permanent establishment or principal place of business within the EU but controlled directly or indirectly by a company outside Europe
- Any company established in Europe that does not comply with the requirements of the law

CULLEN
INTERNATIONAL

Restrictions through spectrum (Nov. 2019)

Authorisation to use/transfer/lease a radio transmitter

Granted only if it can be assumed that the radio use will not harm national security

Combined with specific security requirements related to national security
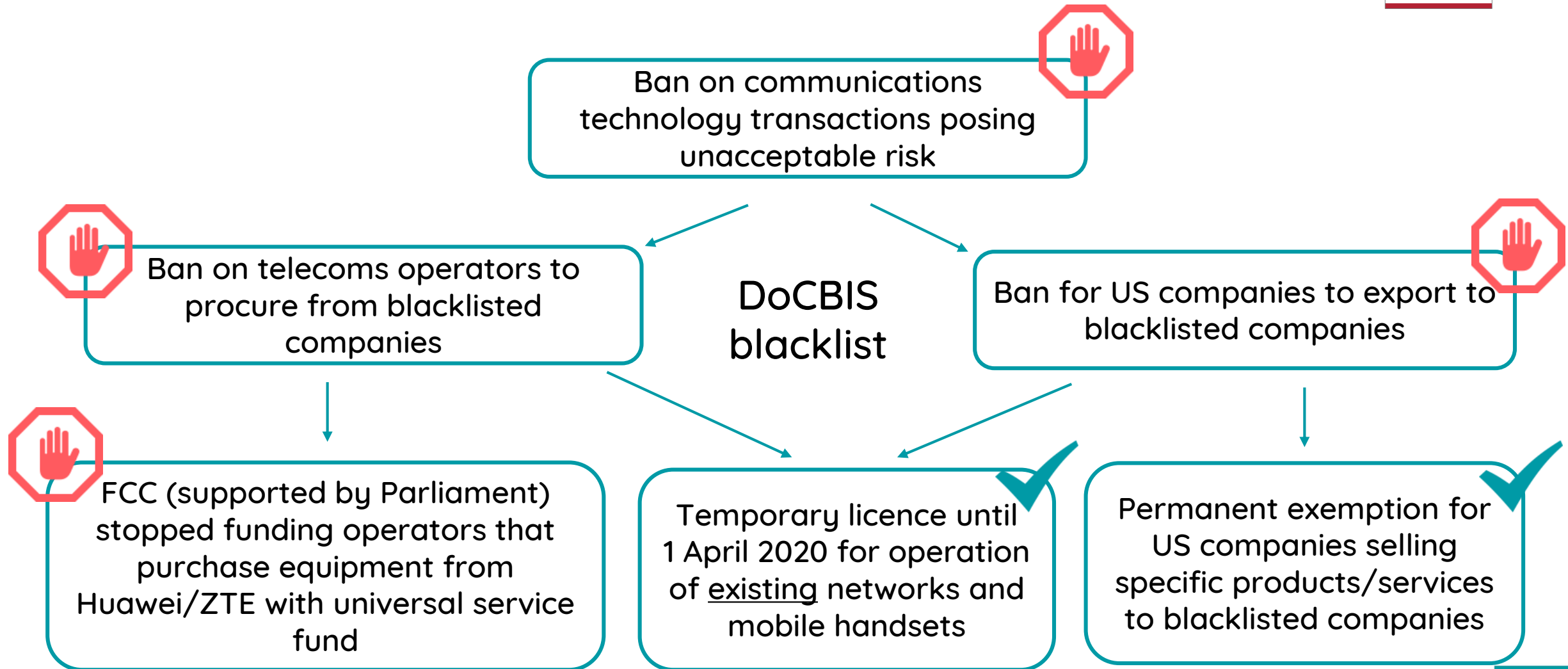
Enforceable from 1 Jan. 2020

BNetzA security catalogue (version 2.0) - pending

ECS/N with increased risk potential, incl. 5G	Mandatory certification of <u>critical components</u>
	Security monitoring
	Proof of trustworthiness of manufacturers and suppliers
	Assurance of product integrity (i.e. through acceptance tests)
	Special requirements for staff with access to safety-relevant areas
	Guarantee of sufficient redundancies
	Avoidance of monocultures

CULLEN
INTERNATIONAL

Trump executive order (May 2019)

Ban on communications technology transactions posing unacceptable risk

Ban on telecoms operators to procure from blacklisted companies

DoCBIS blacklist

Ban for US companies to export to blacklisted companies

FCC (supported by Parliament) stopped funding operators that purchase equipment from Huawei/ZTE with universal service fund

Temporary licence until 1 April 2020 for operation of <u>existing</u> networks and mobile handsets

Permanent exemption for US companies selling specific products/services to blacklisted companies

CULLEN
INTERNATIONAL

5G toolbox – crosscheck

National criteria for high risk suppliers and possibility to restrict

Security standards in procurement
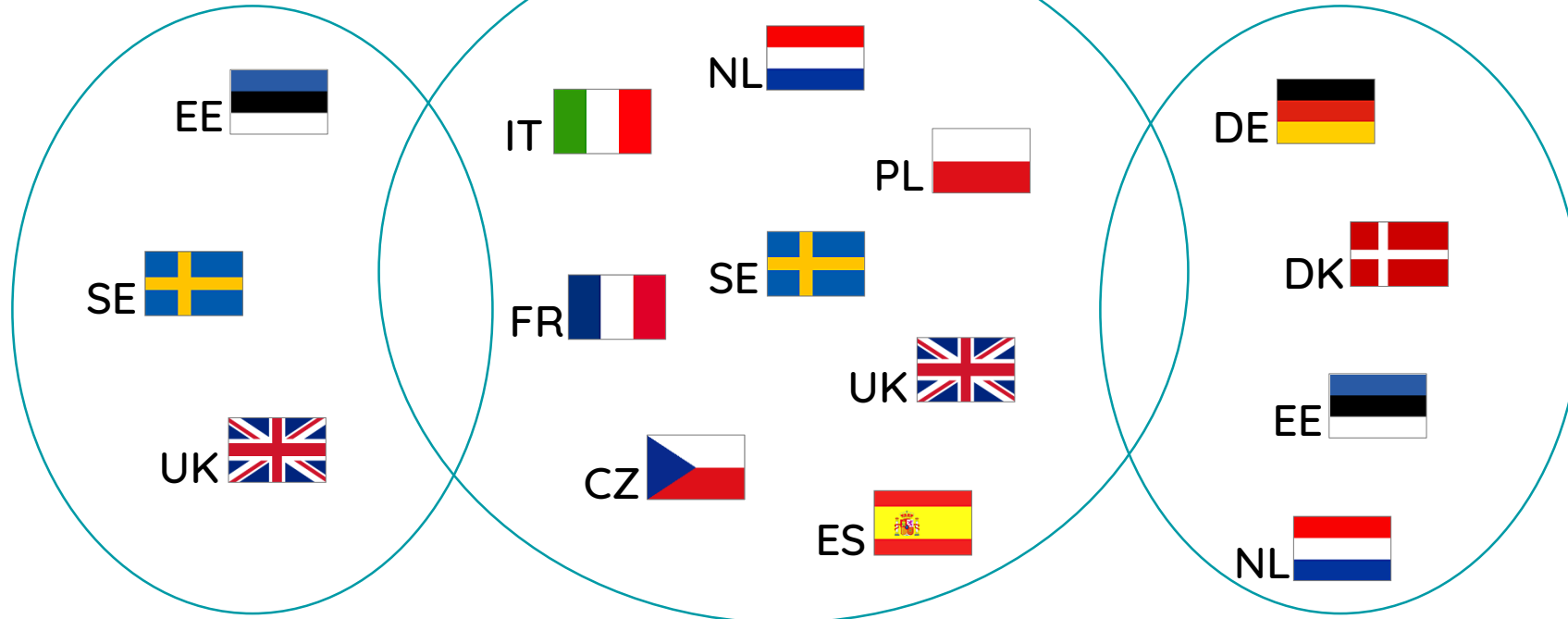
Strick access control

Diversity of suppliers

Certification for critical components in 5G

DK UK

SE

DE

Thank you!

visiola.pula@cullen-international.com