NATIONAL INSTITUTE FOR RESEARCH AND DEVELOPMENT
IN INFORMATICS - ICI BUCHAREST

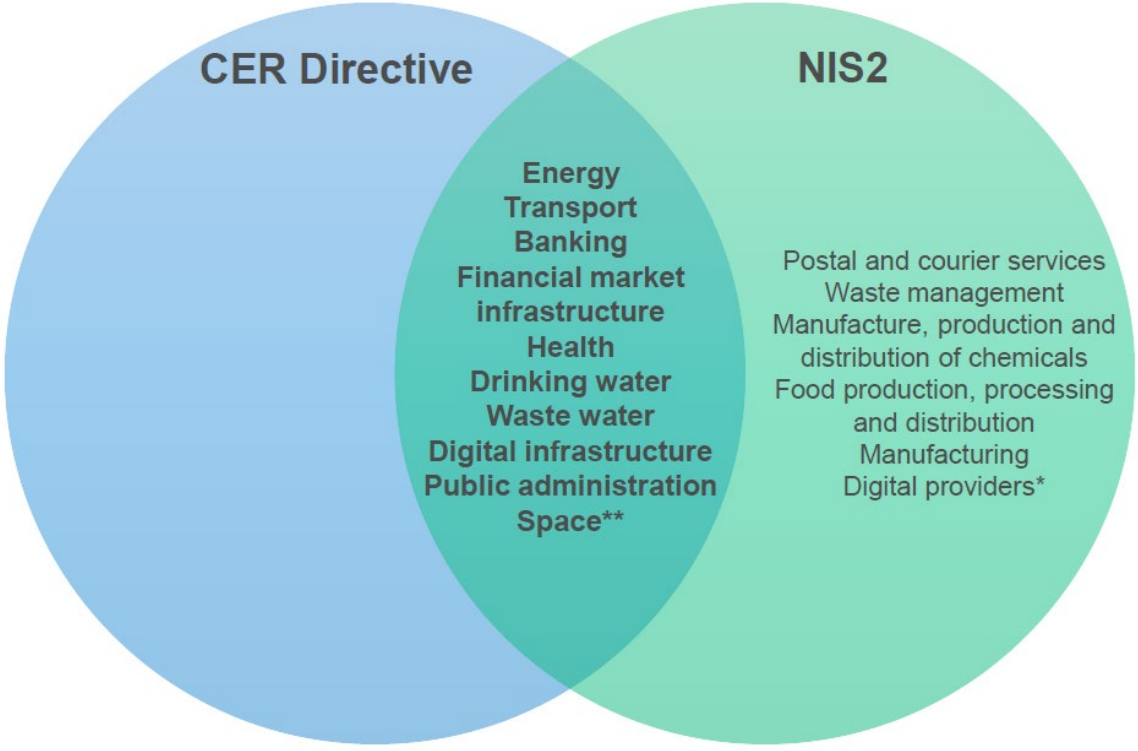
CYBER DIPLOMACY CENTER
ICI Bucharest

Energy Cyber Diplomacy as tool for energy transition

Dr. Carmen-Elena CIRNU
Scientific Director
ICI Bucharest

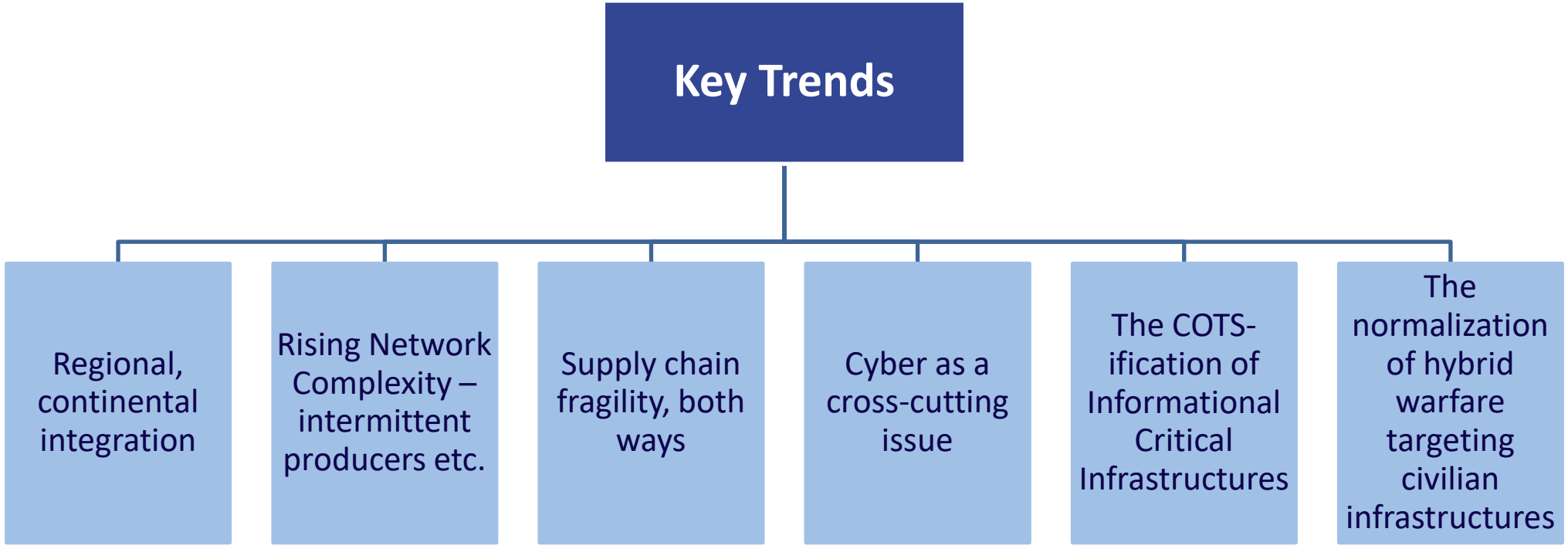
Recent Critical Infrastructure Governance Evolutions in Europe

- The new Critical Entities Resilience Directive and the NIS 2 Directive share a list of critical entity sectors, with energy at the very top
- Critical infrastructures and cyber are inseparable, since cyber is the upper layer of command, control and coordination for all CI



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

Critical Energy Infrastructure Trends



The current cybersecurity environment – trends

- Cyber as a permeating and penetrating factor in **every** critical infrastructure system
- Rise of hybrid warfare and advantages of cyber attacks
- Effects of transborder organized crime
- Commodification of malware
- Blurring of the lines between physical and virtual infrastructure
- Threats outpacing improvements in security culture
- “Proliferation” of cyber weapons and the competence of non-state actors
- **Initial application of new technologies – blockchain and AI – creating new advantages but also risks**
- The mismatch between territorialized state agencies and institutions and cyberspace

What trends can we see for the foreseeable future?

- Systemic effects – more decentralization, less transparency
- Fragmentation of global networks
- Actors deciding to take dramatic steps – going offline, air-gaped systems, the *paperful* office
- AI and cyber are becoming a larger share of the value added of new products and services
- New domains that are underprepared for digitalization – Construction 4.0 etc.
- IoT as a transformative phenomenon on cybersecurity
- New efforts to create a security architecture (norms, agreements etc.) in order to govern the use of cyberattacks between states

What are the possible solutions?

Security Supply

- More investment in cybersecurity tools & research
- Better regulation and homogeneous transborder outcomes
- More coordination and trust building to share info on attacks (including automatically)
- Technical assist. for countries to improve cybersecurity of energy CI

Security Demand

- Investment in cybersecurity culture at organizational level
- Emphasis on cybersecurity in supply chains and interrelated organizations
- Strategic thinking in cyber planning
- Cybersecurity as a mark of competitiveness (market dynamics to reward positive behaviour and punish negligence)

Good Governance
Smart Security
Critical Infrastructure Protection

Cyber Diplomacy, a possible solution

What are the problems addressed by cyber diplomacy?

- Administration of transborder issues arising from the digitization of life, society, the economy and politics
- Cyberattacks are a new weapon of war
- Hybrid warfare and asymmetric warfare
- Targeting civilian infrastructure
- Coordonation on transborder (dis)organized crime
- Administration of global networks, technologies, infrastructure, standards, regulations, conduct etc.
- Collective issue recently discovered – blockchain
- Collective issues not discovered yet

The EU response

An EU "coherent international cyberspace policy"

The vision for the EU's cyber diplomacy was based on the identification of five key priorities:

- the promotion and protection of human rights in cyberspace
- norms of behavior and application of existing international law in the field of international security
- internet governance
- enhancing competitiveness and prosperity
- capacity-building and development

A sixth priority - "strategic engagement with key partners and international organizations" due to the "global cross-cutting nature, scope and reach" of cyber issues

An innovative example - CF SEDSS
European Defence Agency

- Consultation Forum on Sustainable Energy in Defence and Security Sectors

- 4 working groups – energy efficiency, energy transition, **protection of defence-related critical energy infrastructures, transversal working group**

What has CF SEDSS learned?

- There is an important Energy and Defence dimension, where militaries are dependent on civilian energy infrastructures which they do not own, operate or even protect (responsibility of MoI usually)

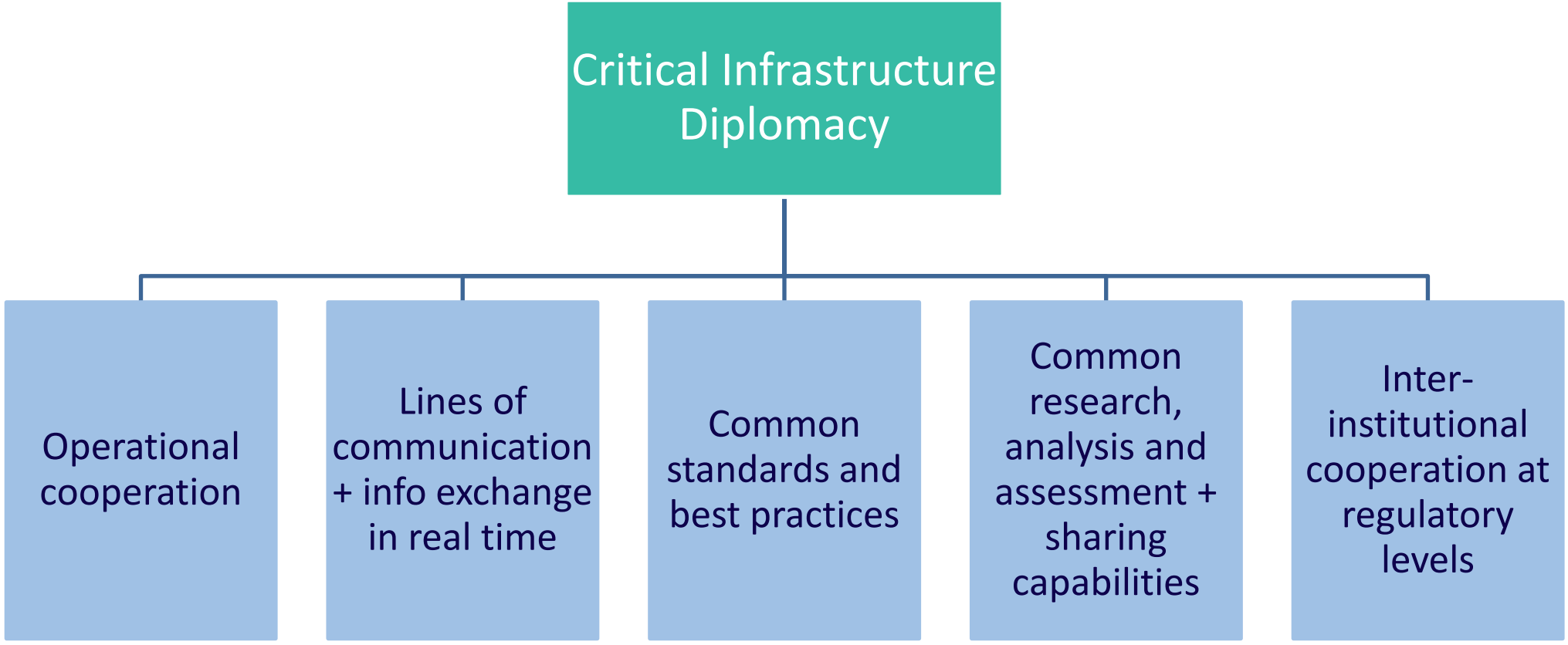
- **Data can be steal from energy providers to extract intelligence regarding military operations**

CIP and Energy Diplomacy

Critical Infrastructure Diplomacy

- It is a pragmatic, risk oriented diplomacy
- Necessity of cooperation between states
- Regardless of geopolitical confrontation, critical infrastructure must be protected and resilient
- The network is only as strong as the weakest link
- Significant risk for cascading disruptions

What does CIP Diplomacy entail?



What can CIP diplomacy achieve now?

- Technical assistance for CIP roadmap, from legislative to personnel and administrative development
- Common security planning sessions for future infrastructures
- Research focus on cross-border infrastructure risks + exercises
- Sharing of capabilities – for instance, ICI Cyber Range
- Security Liaison Office systems for transmission of early warnings and other information
- A reduction in asymmetry of information regarding local infrastructure security environment between states
- More transparency and predictability of transborder CI functioning
- Countermeasures for faster recovery

From the Cyber Diplomat to the Energy Cyber Diplomat

Is there a need for a new role?

Energy Cyber Diplomat

to coordinate protection, security, response and policies for affordability, sustainability and accessibility of energy

CYBER DIPLOMACY CENTER

ICI Bucharest

National Institute for Research and Development in Informatics
ICI Bucharest

carmen.cirnu@ici.ro

WWW.ICI.RO