THE ENERGY COMMUNITY

**Cybersecurity becomes essential,
as teleworking and remote operations increase**

12th OIL FORUM

15 September 2020 - Day 1, Session 1: Oil Security

MAIN AREAS OF WORK

- Statistics
- Electricity
- Renewable energy
- Value added tax
- Competition/state aid
- Environment
- Cyber security
- Regulator
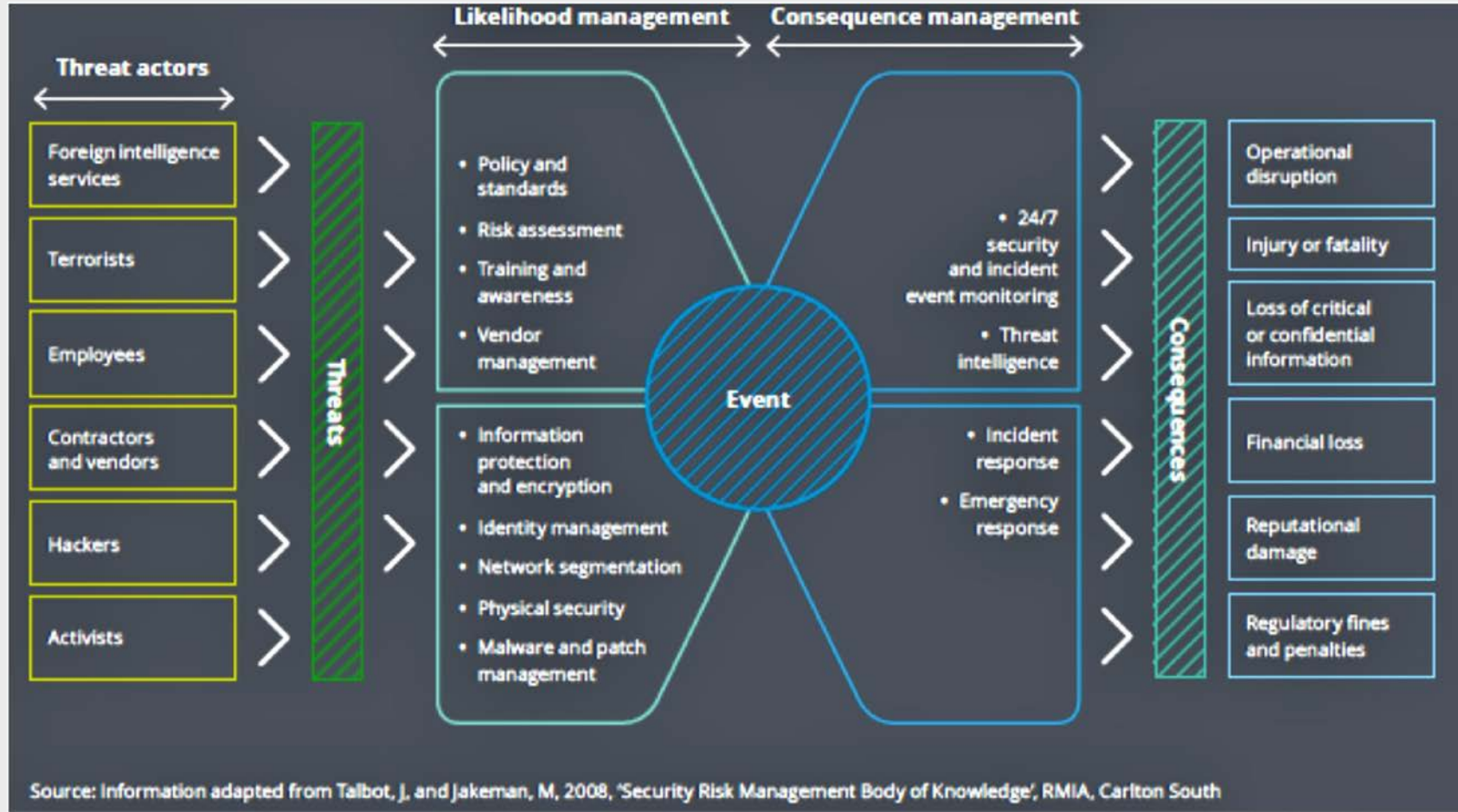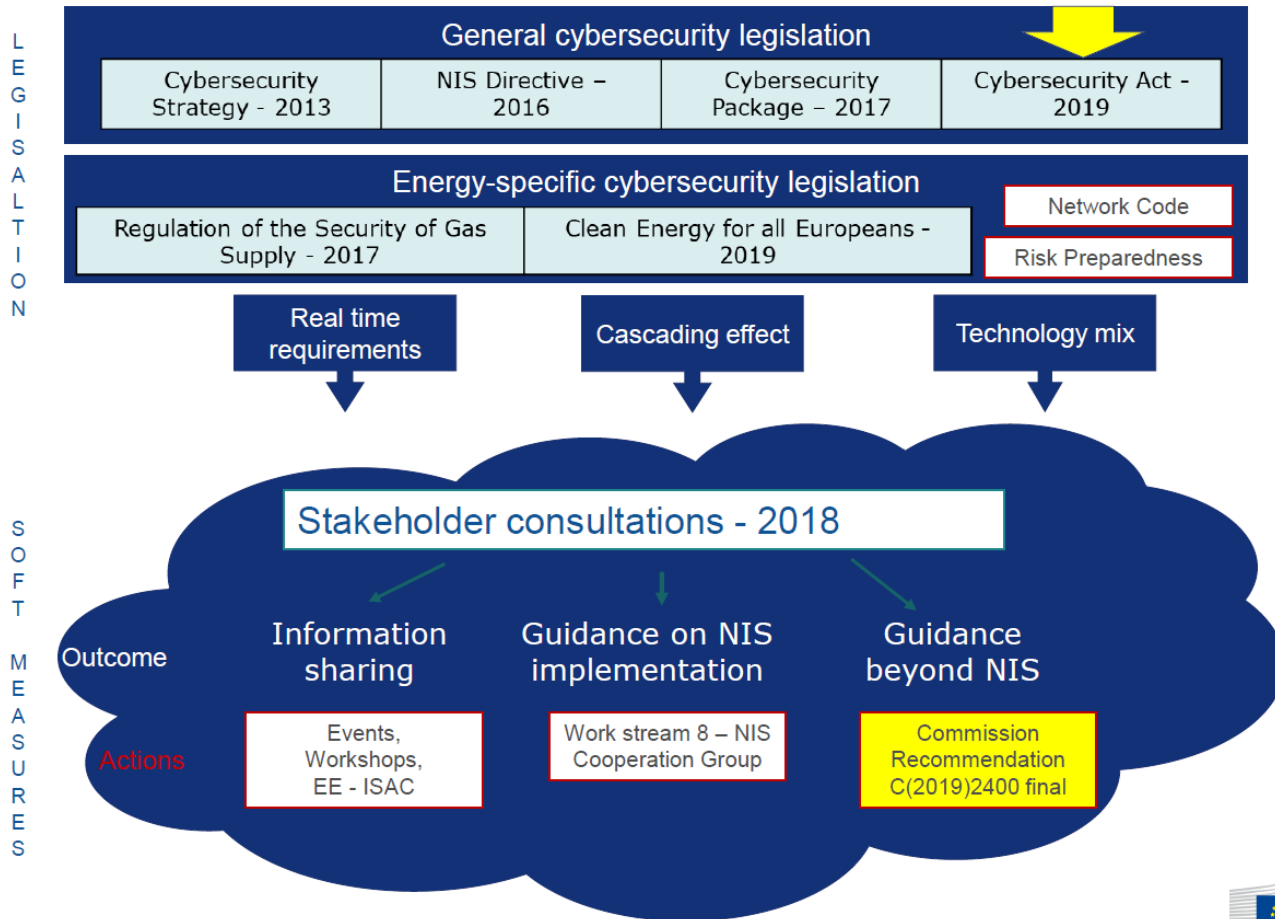- Gas
- Climate
- Energy efficiency
- Oil
- Security of energy supply
- General services

Source: Information adapted from Talbot, J, and Jakeman, M, 2008, 'Security Risk Management Body of Knowledge', RMIA, Carlton South

Energy Community

LEGISALTION

General cybersecurity legislation

Cybersecurity Strategy - 2013	NIS Directive – 2016	Cybersecurity Package – 2017	Cybersecurity Act - 2019

Energy-specific cybersecurity legislation

Regulation of the Security of Gas Supply - 2017	Clean Energy for all Europeans - 2019

Network Code

Risk Preparedness

Real time requirements

Cascading effect

Technology mix

SOFT MEASURES

Stakeholder consultations - 2018

Outcome

Information sharing	Guidance on NIS implementation	Guidance beyond NIS

Actions

Events, Workshops, EE - ISAC	Work stream 8 – NIS Cooperation Group	Commission Recommendation C(2019)2400 final

European Commission

Energy Community

- **PA 2018/02/MC-EnC** (November 2018) on the establishment of Energy Community Coordination Group for Cybersecurity and Critical Infrastructure **(CyberCG)**

Existing EU Legislation

- **ECI** Directive (2008 / 114) on European critical infrastructures
- **NIS** Directive (2016 / 1148) on security of network and information systems
- **EC Recommendation** (2019 / 2400 – April 2019) on cybersecurity in energy
- EU Regulation (2019 / 881) on ENISA technology certification (Cybersecurity act)
- Risk Preparedness Regulation (2019 / 943)

Next generation of cybersecurity acts

- Network Code on Cybersecurity

Cybersecurity – technical standards overview

ISO/IEC 27000

- Information technology security Techniques - 49 items

Other security standards:

- ITU - International Telecommunications Union

- ANSI - American National Standards Institute (USA)

- NIST – National Institute of Standards and Technology (USA)

- **Information Security Management Systems (ISMS)**
  - ISO/IEC 27000:2018   - Overview and vocabulary
  - ISO/IEC 27001:2013   - Requirements
  - ISO/IEC 27002:2013   - Code of practice for information security controls
  - ISO/IEC 27005:2018   - Information security risk management
  - ISO/IEC 27019:2017   - Information security controls for the energy industry

- **Other relevant ISO/IEC standards**
  - ISO/IEC 15408-1:2009   - Evaluation criteria for IT security
  - ISO/IEC 15408-2:2009   - Security functional components
  - ISO/IEC 15408-3:2009   - Security assurance components
  - ISO/IEC 18045:2008   - Methodology for IT security evaluation
  - ISO/IEC TR 19791:2010 - Security assessment of operational systems
  - ISO/IEC 30111:2019   - Vulnerability handling processes

Energy Community Cybersecurity Study – gap analysis

Critical Energy Infrastructures

Legal and Institutional framework

Figure 1: Critical Infrastructure Sectors and Related Sector-Specific Agencies

Chemical [DHS]
Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The sector produces essential products for a range of necessities, including automobiles, pharmaceuticals, food supply, water treatment, and health.

Commercial facilities [DHS]
Protects sites where large numbers of people congregate, such as commercial centers, office buildings, sports stadiums, and theme parks.

Communications [DHS]
Delivers wired, wireless, and satellite communications to meet the needs of business and governments.

Critical manufacturing [DHS]
Alters materials into finished goods, to include manufacture of primary metals, machinery, electrical equipment, appliances and components, and transportation equipment.

Dams [DHS]
Provides support to water retention structures, including levees, dams, navigation locks, canals, and larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.

Defense industrial base [DOD]
Supplies the military with the resources to protect the nation by producing weapons, aircraft, and ships, and provides essential services, including information technology and supply and maintenance.

Emergency services [DHS]
Protects lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.

Energy [DOE]
Delivers the electric power used by all sectors and also includes the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.

Financial services [TREASURY]
Consists of institutions, such as commercial banks, credit unions, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out financial transactions.

Food and agriculture [USDA] [HHS]
Ensures the safety and security of food, animal feed, and food-producing animals; coordinates animal and plant disease and pest response; and provides nutritional assistance.

Government facilities [DHS] [GSA]
Ensures continuity of functions for facilities owned and leased by the government, including all federal, state, territorial, local, and tribal government facilities located in the United States and abroad.

Healthcare and public health [HHS]
Protects the health of the population in the event of a disaster or attack. The sector consists of direct healthcare, health plans and payers, pharmaceuticals, laboratories, blood, medical materials, health information technology, mortuary care, and public health.

Information technology [DHS]
Provides information technology, to include hardware manufacturers, software developers, and service providers, as well as the internet as a key resource.

Nuclear reactors, materials, and waste [DHS]
Provides nuclear power and materials. The sector includes commercial and research nuclear reactors; nuclear fuel fabrication facilities; reactor decommissioning; and the transportation, storage, and disposal of nuclear materials and waste.

Transportation systems [DHS] [DOT]
Provides efficient, safe, and secure freedom of movement for people and commerce across the Nation's transportation systems (aviation, freight rail, highways, maritime, mass transit, motor carriers, pipelines, and postal and shipping).

Water and wastewater systems [EPA]
Provides sources of safe drinking water from community water systems and properly treated wastewater from publicly owned treatment works.

US Government
Accountability Office Report, February 2020

- ECI sectors: energy (Electricity, Gas, Oil), and transport

- Identification of ECI – coordinated criteria
  - Criteria - sectoral, cross-cutting, trans-boundary
  - Thresholds - severity of impact

- Designation of ECI (bilateral / regional)
  - Potential / suspected ECI, level of impact, discussions, reporting (EC), informing the operator, discretion principles

- Operator Security Plan
  - Identification of assets / threat scenarios – risk analysis / vulnerability and potential impact / security measures
  - Periodic review, supervision, community measures and compliance with agreed criteria

- Security Liaison Officers – communication mechanisms

- Threat assessment – reporting, common methodologies, classified information

- An asset, system or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people and the disruption or destruction of which would have significant impact in a MS as a result of the failure to maintain those functions

- significant impact on at least two MSs (CPs)

- Build sufficient resilience capacity at national level
  - Adopt a national NIS strategy
  - Designate national cybersecurity authorities, single contact points and Computer Security Incident Response Teams (CSIRTs)

- Identify critical infrastructure, operators of essential services (OES), and relevant digital service providers

- Build structures for cross-border cooperation and exchange of information
  - At strategic level - creating a Cooperation Group of national authorities
  - At operational level - creating a network of national CSIRTs

- Cumulative conditions for identification of OES
  - Service essential for societal / economic activities, depends on network and information systems, an incident would have significant disruptive effects

- Security and notification requirements imposed on OES

- Monitoring and enforcement powers

a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;

b) the provision of that service depends on network and information systems; and

c) an incident would have significant disruptive effects on the provision of that service.

Energy Community

- EC Recommendation C(2019)2400,
- Staff Working Paper SWD(2019)1240 :

- **Real-time requirements** (**IT** and **OT**) - some energy systems need to react so fast that standard security measures such as authentication of a command or verification of a digital signature can simply not be introduced due to the delay these measures impose.

- **Cascading effects** - electricity grids and gas pipelines are strongly interconnected across Europe and well beyond the EU. An outage in one country might trigger blackouts or shortages of supply in other areas and countries.

- **Combined legacy systems with new technologies** - many elements of the energy system were designed and built well before cybersecurity considerations came into play. This legacy now needs to interact with the most recent state-of-the-art equipment for automation and control, such as smart meters or connected appliances, and devices from the Internet of Things without being exposed to cyber-threats.

Real-time Requirements

- Use international standards
- Apply physical measures
- Classify / manage your assets
- Consider privately owned communication networks, or consider specific measures
- Consider splitting systems into logical zones
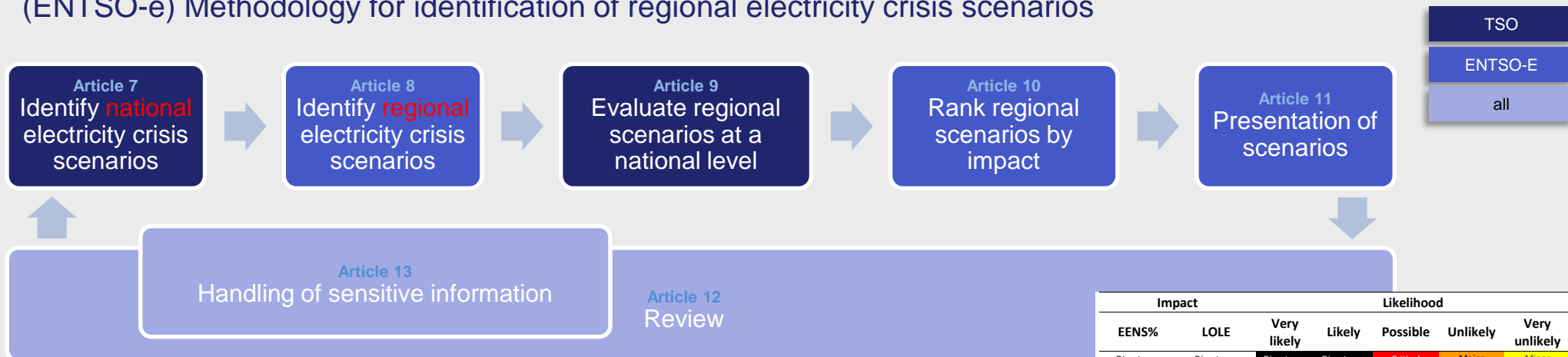- Choose secure communication and authentication

Cascading effects

- Evaluate interdependencies
- Ensure communication framework for early warnings and to cooperate in crisis
- Ensure level of security for new devices
- Consider cyber - physical spill overs
- Establish design criteria for a resilient grid

Technology mix

- Follow a cybersecurity-oriented approach when connecting devices
- Use international standards
- Establish monitoring and analysis capabilities
- Conduct specific cybersecurity risk analysis for legacy installations
- Collaborate with technology providers
- Update hardware and software

Energy Community

(ENTSO-e) Methodology for identification of regional electricity crisis scenarios

TSO
ENTSO-E
all

Article 7 Identify national electricity crisis scenarios → **Article 8** Identify regional electricity crisis scenarios → **Article 9** Evaluate regional scenarios at a national level → **Article 10** Rank regional scenarios by impact → **Article 11** Presentation of scenarios

Article 13 Handling of sensitive information

Article 12 Review

Classification	Events per year	1 x in … years	Description/example of initiating event
Very likely	≥ 0.5	2 or less	event expected practically every year, e.g. extreme winds/storms causing multiple failures of overhead lines may be expected nearly every year in some areas
Likely	0.2-0.5	2-5	event expected once in a couple of years, e.g. extreme heat wave causing limits on output of open-loop water-cooled power plants, low water levels at hydro plants, higher load, etc.
Possible	0.1-0.2	5-10	event expected or taken into consideration as a potential threat, e.g. cyber or malicious attack
Unlikely	0.01-0.1	10-100	very rare event with potentially huge impact, e.g. simultaneous floods causing unavailability of generation, distribution and transmission infrastructure
Very unlikely	≤ 0.01	100 or more	event not observed but potentially disastrous, e.g. earthquake causing a huge destruction of transmission, distribution and generation infrastructure

Classification	EENS%* (of annual demand)	LOLE* [hours]
Disastrous	≥0,25%	≥168
Critical	≥0,05% and <0,025%	≥48 and <168
Major	≥0,01% and <0,05%	≥12 and <48
Minor	≥0,002% and <0,01%	≥3 and <12
Insignificant	<0,002%	<3

Impact		Likelihood				
EENS%	LOLE	Very likely	Likely	Possible	Unlikely	Very unlikely
Disastrous	Disastrous	Disastrous	Disastrous	Critical	Major	Minor
Disastrous	Critical	Disastrous	Critical	Critical	Major	Minor
Critical	Disastrous	Disastrous	Critical	Critical	Major	Minor
Disastrous	Major	Disastrous	Critical	Major	Major	Minor
Major	Disastrous	Disastrous	Critical	Major	Major	Minor
Disastrous	Minor	Disastrous	Critical	Major	Major	Minor
Minor	Disastrous	Disastrous	Critical	Major	Major	Minor
Disastrous	Insignificant	Disastrous	Critical	Major	Major	Minor
Insignificant	Disastrous	Disastrous	Critical	Major	Major	Minor
Critical	Critical	Disastrous	Critical	Major	Minor	Minor
Critical	Major	Critical	Critical	Major	Minor	Minor
Major	Critical	Critical	Critical	Major	Minor	Minor
Critical	Minor	Critical	Major	Major	Minor	Minor
Minor	Critical	Critical	Major	Major	Minor	Minor
Critical	Insignificant	Critical	Major	Major	Minor	Minor
Insignificant	Critical	Critical	Major	Major	Minor	Minor
Major	Major	Critical	Major	Major	Minor	Insignificant
Major	Minor	Major	Major	Minor	Minor	Insignificant
Minor	Major	Major	Major	Minor	Minor	Insignificant
Major	Insignificant	Major	Major	Minor	Minor	Insignificant
Insignificant	Major	Major	Major	Minor	Minor	Insignificant
Minor	Minor	Major	Minor	Insignificant	Insignificant	Insignificant
Minor	Insignificant	Major	Minor	Minor	Insignificant	Insignificant
Insignificant	Minor	Major	Minor	Minor	Insignificant	Insignificant
Insignificant	Insignificant	Minor	Minor	Insignificant	Insignificant	Insignificant

Overall risk assessment (electricity / gas)

- Priority in terms of likelihood and impact

- Range according to type of threat

- Distribution according to type of stakeholder

	Cyber Threat							
	Malware	**Web Based Attacks/Web application attacks**	**Social engeneering/Phising/Spam**	**Denial of Service (DoS)**	**Insider Threat**	**Cyber Espionage Cyberwarfare**	**Ransomware**	**Botnet**
NRA	MEDIUM RISK for CA/NRA · LOW RISK in cascading effect to other energy stakeholder	NOT APPLICABLE for CA NRA	HIGH RISK for CA/NRA · MEDIUM RISK in cascading effect to other energy stakeholder	HIGH RISK for CA/NRA · LOW RISK in cascading effect to other energy stakeholder	HIGH RISK for CA/NRA · HIGH RISK in cascading effect to other energy stakeholder	CRITICAL RISK for CA/NRA · HIGH RISK in cascading effect to other energy stakeholder	MEDIUM RISK for CA/NRA · MEDIUM RISK in cascading effect to other energy stakeholder	MEDIUM RISK for CA/NRA · LOW RISK in cascading effect to other energy stakeholder
TSO	HIGH RISK for TSO · MEDIUM RISK in cascading effect to other energy stakeholder	MEDIUM RISK for TSO · LOW RISK in cascading effect to other energy stakeholder	HIGH RISK for TSO · HIGH RISK in cascading effect to other energy stakeholder	LOW RISK for TSO · LOW RISK in cascading effect to other energy stakeholder	HIGH RISK for TSO · HIGH RISK in cascading effect to other energy stakeholder	HIGH RISK for TSO · HIGH RISK in cascading effect to other energy stakeholder	HIGH RISK for TSO · HIGH RISK in cascading effect to other energy stakeholder	HIGH RISK for TSO · HIGH RISK in cascading effect to other energy stakeholder
DSO	MEDIUM RISK for DSO · MEDIUM RISK in cascading effect to other energy stakeholder	MEDIUM RISK for DSO · LOW RISK in cascading effect to other energy stakeholder	HIGH RISK for DSO · MEDIUM RISK in cascading effect to other energy stakeholder	LOW RISK for DSO · LOW RISK in cascading effect to other energy stakeholder	MEDIUM RISK for DSO · LOW RISK in cascading effect to other energy stakeholder	HIGH RISK for DSO · MEDIUM RISK in cascading effect to other energy stakeholder	HIGH RISK for DSO · HIGH RISK in cascading effect to other energy stakeholder	HIGH RISK for DSO · MEDIUM RISK in cascading effect to other energy stakeholder
Genco	LOW RISK for Generation · MEDIUM RISK in cascading effect to other energy stakeholder	LOW RISK for Generation · LOW RISK in cascading effect to other energy stakeholder	MEDIUM RISK for Generation · LOW RISK in cascading effect to other energy stakeholder	LOW RISK for Generation · MEDIUM RISK in cascading effect to other energy stakeholder	MEDIUM RISK for Generation · LOW RISK in cascading effect to other energy stakeholder	MEDIUM RISK for Generation · MEDIUM RISK in cascading effect to other energy stakeholder	HIGH RISK for Generation · MEDIUM RISK in cascading effect to other energy stakeholder	MEDIUM RISK for Generation · MEDIUM RISK in cascading effect to other energy stakeholder
PX	LOW RISK for Exchange · LOW RISK in cascading effect to other energy stakeholder	LOW RISK for Exchange · LOW RISK in cascading effect to other energy stakeholder	LOW RISK for Exchange · LOW RISK in cascading effect to other energy stakeholder	LOW RISK for Exchange · LOW RISK in cascading effect to other energy stakeholder	LOW RISK for Exchange · LOW RISK in cascading effect to other energy stakeholder	LOW RISK for Exchange · LOW RISK in cascading effect to other energy stakeholder	MEDIUM RISK for Exchange · LOW RISK in cascading effect to other energy stakeholder	LOW RISK for Exchange · LOW RISK in cascading effect to other energy stakeholder

Energy Community Cybersecurity Study – inherent risk pattern

Energy Community Cybersecurity Study – inherent risk assessment

Albania

Bosnia and Herzegovina

Georgia

Kosovo*

Moldova

Montenegro

North Macedonia

Serbia

Ukraine
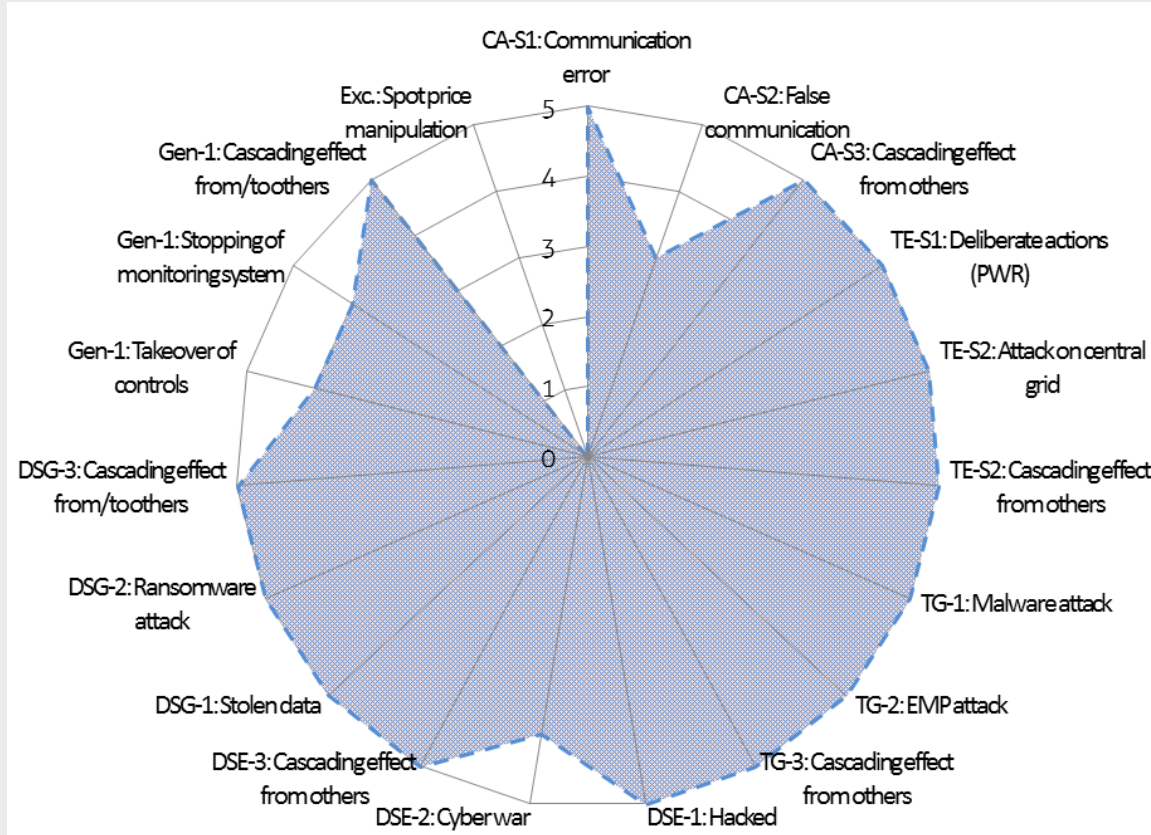
General recommendations for Ministries

o Start as soon as possible with the implementation of the legal framework and provide sufficient budgetary resources during implementing laws, legal documents and strategies.

o Organize a sector specific CSIRT (or allocate sufficient resources in existing CSIRT infrastructure to address energy- specific incidents in real time)

o Establish an online communication channel to enable reporting and feedback line with all members of the energy sector.

o Establish a system for early warning and exchange of information on cyber threats / provision of assistance in energy.

o Conduct a standardized, overall sector specific risk assessment for the country based on the collected relevant information about assets, vulnerabilities and threats (including cascading, cross sectorial and cross-border risks).

o Ensure that newly discovered risks are managed through enforcing TSOs and DSOs in implementing action plans and controlling the management process.

o If appropriate, for the smaller DSOs, generators or new type of market participants the organize a national ISAC as a source of information, analysis and remediation solutions.

General recommendations for NRA / Liaison officers

o The cybersecurity Liaison officer must have a complete understanding of local energy stakeholders, market, critical infrastructure protection and their capability to handle the most complex issues in information and cybersecurity. They would serve as a focal point between EnC CyberCG / NRA Working stream and local operational entities

o NRAs should serve as a central monitoring hub in controlling the exchange of critical infrastructure protection and cybersecurity related information.

o The capability to be supported by NRA own employees which must have international certifications in the field of information and/or cyber security (CISA, CISM, CISSP, ISO27LA).

o The local NRAs must have the capability to master the EU Critical Infrastructure Protection and NIS directive related issues and also have power to enforce changes in local energy sector regulation regarding the same.

o The local NRAs must have power to supervise by controls and/or audit the NRA licensed companies for cyber security issues in order to enforce the managing of risks on required level.

Main areas (working groups)

Critical Energy Infrastructures / Essential Services

- Update on the State of affairs / recommendations / benchmark on the applied criteria (EnC) – follow-up on the Study
- Common guidelines on the regional criteria for designation (ECS)
- Risk Preparedness Regulation (methodology) – (EC, ENTSO-e / ECS)

Legal framework (governance) – ECI Directive, NIS Directive

- Guidelines / roadmap for (early) implementation (ECS / TA)
- Cybersecurity Network Code (draft - EC)
- ECRB – application of technical standards for Cybersecurity (ToR – ECS / TA)

Energy Community ISAC (CSIRT network)

- White Paper, ToR, roadmap (ECS)
- Initial group of stakeholders (establishment) – (EnC)

Cybersecurity Academy

- Training seminars / workshops (ECS / TA)

Establishment

Administrative & legal format

- An international association under the Austrian law – ToR, roadmap (ECS)
- Legal acts (AA), local legislation, enforcement, penalties
- Financing

Membership

- Members – criteria for participation, scope, restrictions
- Partners

Meetings and events

- Representatives
- Chairperson, Board
- Working groups, projects
- Role of the ECS
- Common projects (Working groups) on mutual domains of interest

Energy Community ISAC

Operation

Information sharing

- Classification and restricted access (WHITE / GREEN / AMBER / RED)
- Confidentiality memorandum (statement) – obligation for non-disclosure
- Publication (transparency) – regulated and coordinated

Mutual assistance and activities

- Exchange / analysis of sensitive information – direct added value, trusted environment
- Sharing human capacity / cooperation within the CSERT community
- Coordinated standards / best practices
- Partnership relations - ISACs in other regions / sectors, EU associations / authorities, public sector
- Common projects (Working groups) - mutual domains of interest
- Publications, external events

Training

- Forensic training sessions, education on risk assessment and remedies
- Specific case analysis, security plans and training exercises

Activities & Sharing Topics

Physical Info Sharing Community	Digital Info Sharing Community	Topics of Information Sharing
• Plenary meetings • Community meetings • Theme based meetings • Open house meetings	• Information requests / push • Webinars • Whitepaper	• Vulnerabilities in OT systems and critical assets • Threat/Risk analysis information • Incidents • Lessons learned / best practices • Alerts and (patch)notifications • Use of standards (ISO, IEC, NIST, NERC etc.) • Research (H2020) topics

EE-ISAC

THANK YOU for your kind attention

simon.uzunov@energy.community.org

🌐 www.energy-community.org

🐦 Ener_Community

in /company/energy-community

f /Ener.Community

▶ /EnergyCommunityTV