Study on Cybersecurity in the energy sector of the Energy Community

Workshop #2
Workshops 2-1 and 2-2

Blueprint Energy Solutions GmbH

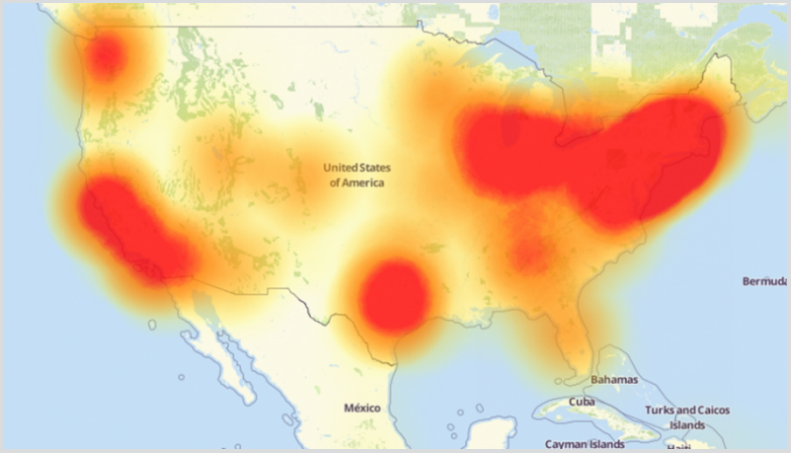
Presenters:
Peter Grasselli - CISA, CISSP
Szabolcs Hallai, CISA, CISM, CITRM, C|CISO, C-DPO

Vienna, 17.09.2019.

Introduction

- Introduction
- WS2-1 „Criteria for identification of large-scale cybersecurity Incidents“
- WS 2-2 „Designing the action plans for EnC Contracting Parties“

Some large-scale cyber attacks



Botnets

- Noname, 2019, 850.000 dev
- Mirai, 2016, 300.000 dev
  DDOS attacks, DynDNS indirectly AirBnB, GitHub, Twitter, Reddit, Netflix and others

Ransomware

- LockerGoga, 2019
  Norsk Hydro, Hexion, Momentive, Altran Technologies, …
- WannaCry, 2017
  O2, Honda, Renault, Dacia, National Health Service of England and Scotland, …
  Cumulative damage 4-8 billons $
- NotPetya, 2017
  Energy companies, power grid, gas stations, banks, …
  US White House assessment of damage 10 billion $

DDOS, Estonia, 2007

Estonian Parliament, Banks, Ministries, Newspapers, broadcasters, …

Some energy-specific cyber attacks

Jul 2019 City Power Johannesburg - ransomware

Attacks against City Power left residents of Johannesburg without electricity up to 12 hours as all databases, applications, prepaid vending system and networks have been encrypted. The malware prevented users from buying electrical power units or feeding/selling electricity into the grid. It is unclear which ransomware is behind the attack. The company managed to restore its operation from backups.

Dec 2015 Saudi Arabia, United Arab Emirates oil industry - Shamoon

Malware targeting oil and gas industry organizations with intent to disable operations. Shamoon is a self-propagating wiper malware transferring itself through a list of remote computers, acquired by reconnaissance conducted before the infection. Once the devices are infected it triggers payload to delete files on the hard drive and deletes master boot record rendering the machine unusable and data unrecoverable.

Dec 2015 Ukraine cyber-attack on power grid; Prykarpattyaoblenergo & Chernivtsioblenergo

Being regarded as first successful cyber-attack on a power grid, it caused up to 6 hours of disruption in electricity supply to a geographical area of 230,000 people.

Dec 2016 Crashovveride - Ukraine

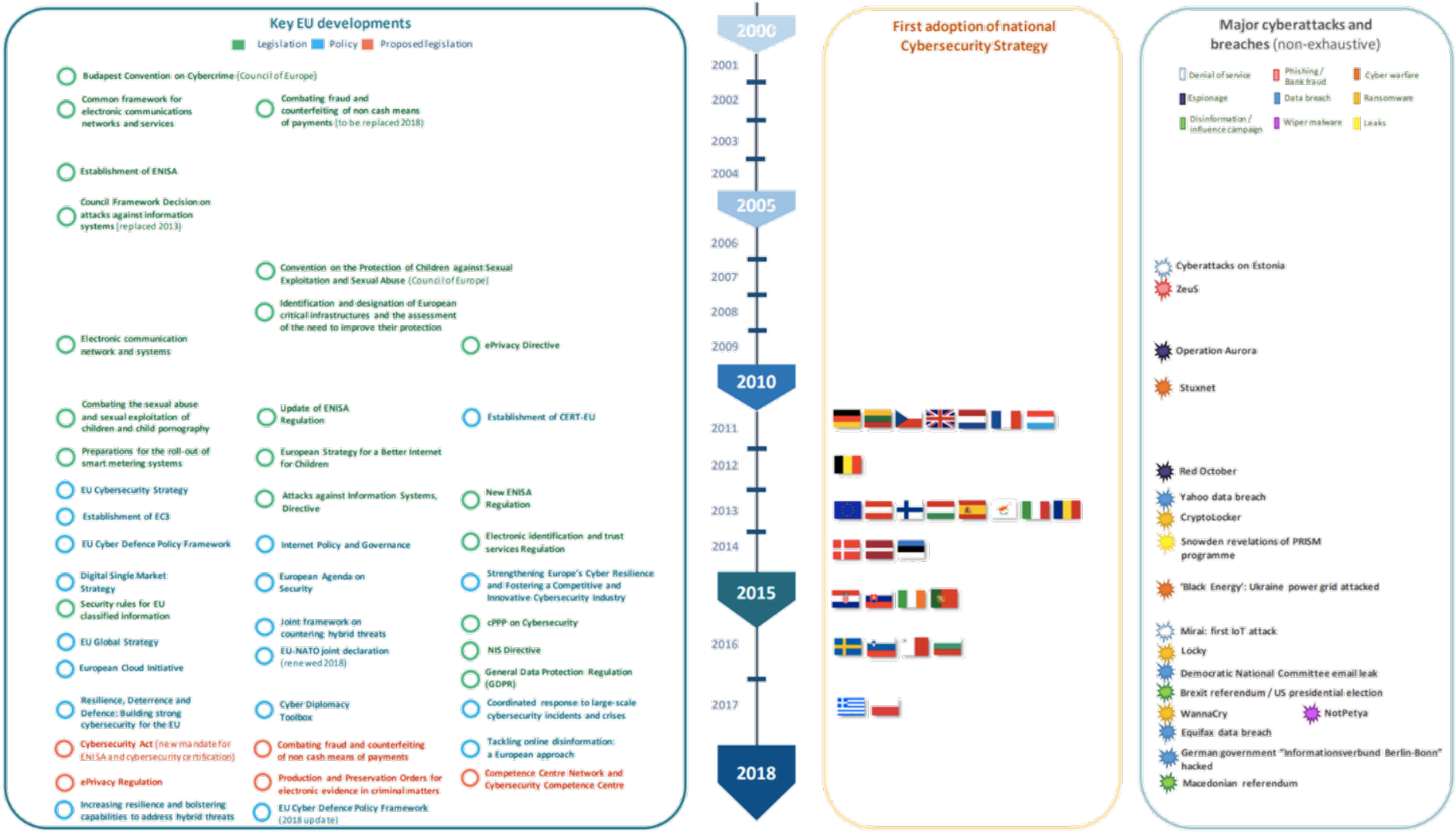
Lessons Learned

Cyber-attacks more common and dangerous
Anonymity and deniability of the cyberspace
Militarization of cyber space

- (Auto)patch and update
- Principle of least privilege
- Eliminate default credentials, use strong credentials
- Disable listening/update mechanism on ICS/SCADA
- Disable remote access to ICS/SCADA or separate IT/OT
- Close specific ports (445)
- Disabling automatic macro-loading in Office suite
- Monitoring of networks
- Backup essential information, airgap/offline backups
- Implement rate-limiting
- Secure email gateways
- Develop security culture
- Develop cyber-security response units

There is no silver bullet: *Layer/defence in depth*
principles and multiple security levels
Implementation of security measures

Overview of EU activities



Source: ECA.

Study on Cybersecurity in the energy sector of the Energy Community

WS2-1 Criteria for identification of large-scale cybersecurity incidents

Blueprint Energy Solutions GmbH

Presenter:
Peter Grasselli - CISA, CISSP

Vienna, 17.09.2019.

Agenda

- Large-scale cybersecurity incident definition
- Criteria development – where to start
  - EU legislation provisions
  - Examples of CI/ES criteria
- Methodologies overview
- Case study

Cyber security incident

Any occurrence that has impact on any of the components of the cyber space or on the functioning of the cyber space, … *ENISA 2017*

An event that directly or indirectly harms or threatens the resilience and security of an IT system and the data it processes, stores or transmits. *ECA 2018*

Single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security *ISO 27000:2018*
Event: Occurrence or change of particular set of circumstances Difference between cyber security and information security

Unlike a breach, a cyber security incident doesn't necessarily mean information is compromised; it only means that information is threatened.

Large-scale cybersecurity incident

Cybersecurity incident which:

- cause disruption too extensive for a concerned Member State to handle on its own or
- which affect two or more Member States or EU Institutions with such a wide-ranging and significant impact of technical or political significance that they require timely policy coordination and response at Union political level.

Commission recommendation on coordinated Response to Large Scale Cybersecurity Incidents and Crises

Need for criteria

- Cybersecurity threats are global in nature
- Cyber incidents information sharing increase probability and speed of prevention/response
- Sector specific information is of great importance for prevention and timely response
- Cross-border impacts

BUT

- Trust is a prerequisite
- What is/could be large scale incident for one party is not necessary for others
- Ex-ante or ex-post criteria
- Scope of information sharing

CI criteria (ECI)

- **casualties criterion** (assessed in terms of the potential number of fatalities or injuries);
- **economic effects criterion** (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects);
- ***public effects criterion*** *(assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services)*

Thresholds determined on case-by-case basis by states concerned

ES criteria (NIS)

- an entity provides a service which is essential for the maintenance of critical societal and/or economic activities
- the provision of that service depends on network and information systems
- an incident would have significant **disruptive effects** on the provision of that service

Significant disruptive effect criteria

- the number of users relying on the service provided by the entity concerned
- the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety
- the market share of that entity
- the geographic spread with regard to the area that could be affected by an incident
- the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

Methodologies

Non exhaustive list of methodologies:

- Methodologies for the identification of Critical Information Infrastructure assets and services *ENISA, 2014*
- ISO 31000:2018 Risk management – Guidelines
- ISO 27005:2018 Information technology -- Security techniques -- Information security risk management
- European Risk Assessment and Contingency planning Methodologies (EURACOM) *FP7-financed Coordination Action, addresses the issue of protection and resilience of energy supply for European interconnected energy networks, 2011*
- SEGRID Risk Management Methodology (SRMM) *EU FP7 SEGRID project, 2017*

CI/ES criteria examples EU

	Electricity		Gas		Population (mio)
MS	Customers	Generation/ Transmission	Customers	Generation/ Transmission/Storage	
DE	3.700 GWh/year	420MW	5.190 GWh/year	5.190 GWh/year	82
GB*	250.000	2GW	250.000	20 Mio m3/day	66
NL*	8.000	350MW	2.000		17
SI	100.000/3 days	7 days grid blackout	100.000/1 week		2

*Criteria encompass relevant license

EU example – Significant disruptive effect

Dependencies between CIs through assessment for category A CI and ES: (DEFINED FOR STATE WIDE Energy)

- Physical impact is greater than 10,000 casualties, serious wounded or chronically ill
- Economic impact is greater than 50,000 million euro, or 5% decrease in real income on state level
- Social-psychological impact is greater than 1 million persons emotionally affected or experience serious societal survivability problems
- Cascade impact disrupts or causes failure in two other critical sectors

EU example – Significant disruptive effect

Category B (DEFINED FOR REGIONAL DISTRIBUTION of Energy)

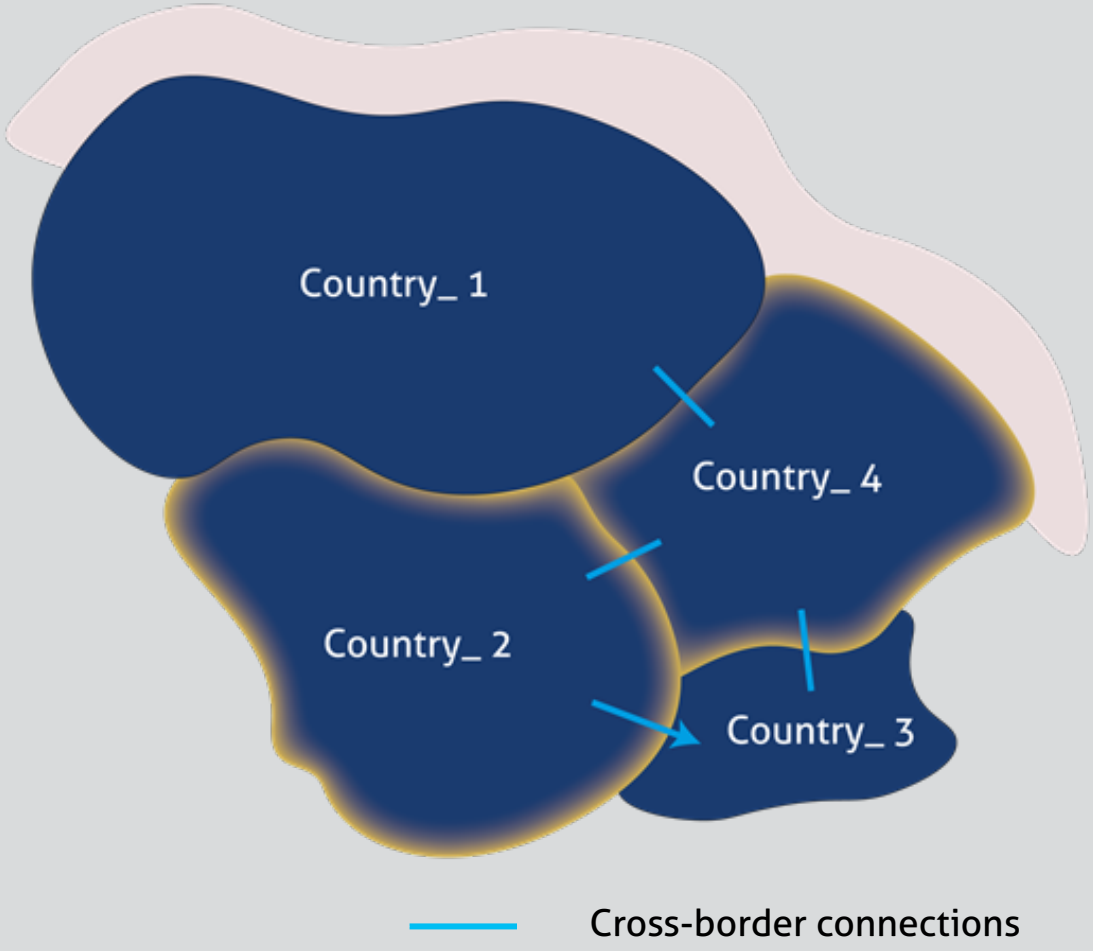
- Physical impact is greater than 1,000 casualties, serious wounded or chronically ill
- Economic impact is greater than 5,000 million euro, or 1% in decrease in real income
- Social-psychological impact is greater than 100,000 persons emotionally affected or experience serious societal survivability problems

EnC examples

- More than 39.000 individuals are influenced
- Incident causes disconnection for intervals longer than 24 hours
- Financial impact is more than 30.000 EUR

- More than 10.000 individuals are affected
- Disruption and recovery activity lasting more than 6 months
- Economic impact is more than 5 million EUR

CASE STUDY SECNARIO



Country_1, Enc CP, large population

Country_2, EU MS, approx. Half the Country_1 population

Country_3, EnC CP, small population (relatively to other countries)

Country_4, EU MS, population similar to Country_2

CASE STUDY SECNARIO

A new type of hybrid crypto-ware developed by state sponsored groups designed to disable (e.g. encrypt-ransomware) SCADA systems in the energy sector is used to attack Country_1.

Country_1 successfully deals with the attack (in the past being engaged in hybrid war) however malware is propagated by email communication between mail correspondence to Country_2, Country_3 and Country_4 TSO/DSO SCADA systems.

Contry_2 relatively successfully mitigate attack with minor impact due to organisational and technical controls established in scope of Cybersecurity action plan that was developed and implemented based on the critical infrastructure and essential services related legislation (transposition of ECI and NIS in local legislation).

Country_4 also successfully mitigate attack due to the response structures established in the past as a consequence of on-going cyber-attacks on the country.

Country_3 is geo-political neutral and as such did not have experience with targeted cyberattack campaigns. Although majority of ECI/NIS provisions were already transposed into the local legislation the implementation of organisational and technical controls is in early stages. As a consequence, Contry_3 suffers major outages resulting in declaration of emergency state and political turmoil.

Study on Cybersecurity in the energy sector of the Energy Community

WS2-2 Designing the action plans for EnC Contracting Parties

Blueprint Energy Solutions GmbH

Presenter:
Szabolcs Hallai, CISA, CISM, CITRM, C|CISO, C-DPO

Vienna, 17.09.2019.

Agenda

- Introduction
- Overview of EU measures and analyzing them
- How to design an action plan
- Sample plan

Introduction

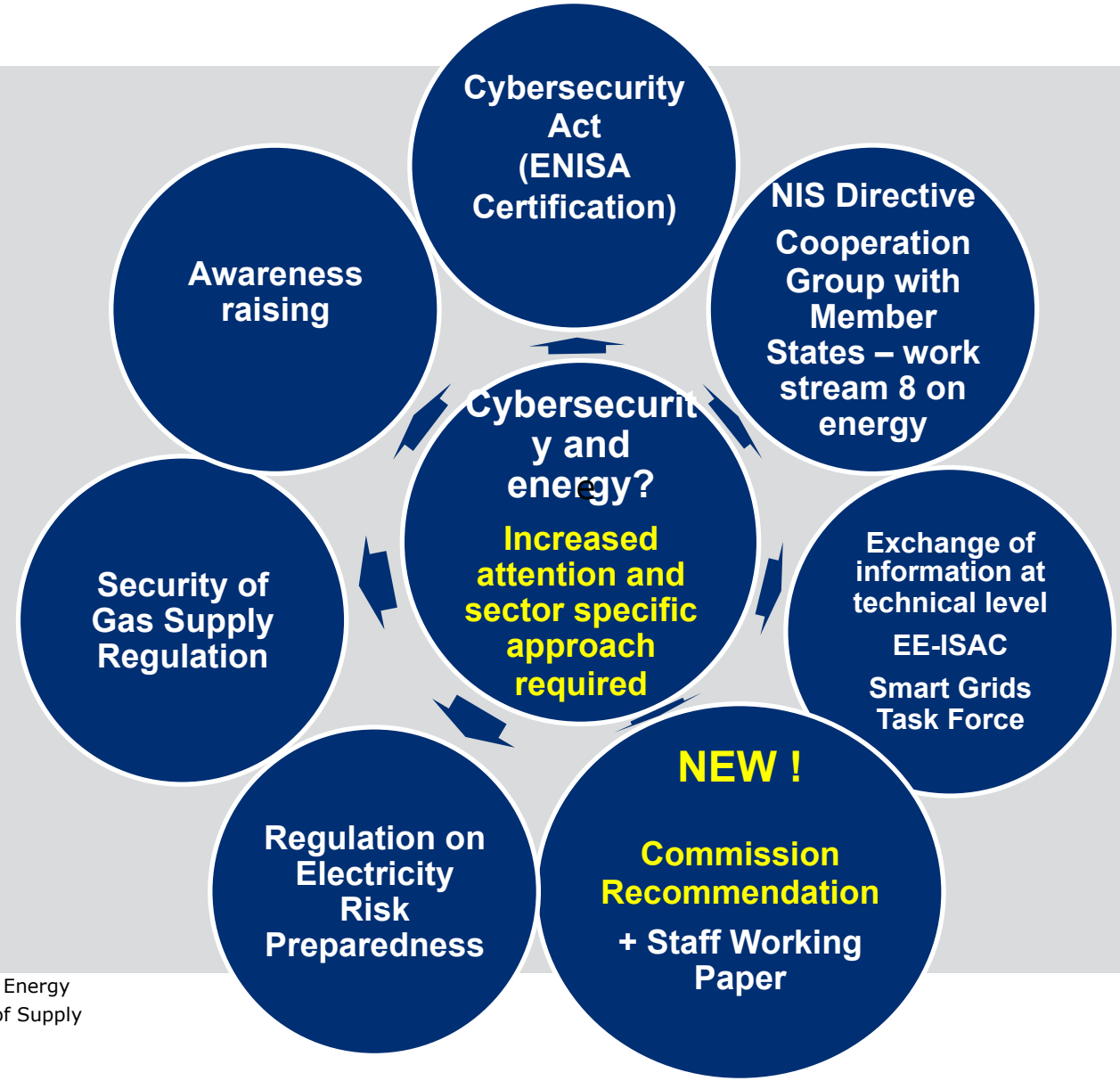
We just finished a workshop about large scale cybersecurity incidents.

During that workshop we gain an awareness about incidents and their possible impacts on stakeholdrers.

It is time to create an action plan to succesfully mitigate the cybersecurity risks.

At the end of this presentation we will divide into two groups (Legal framework, operational) to create a sample action plan for a baseline country. Groups will be led by Blueprint Energy experts

Overview of EU measures and analyzing them



Source: Rémi Mayet
Directorate General for Energy
Deputy Head Security of Supply
European Commission

Overview of EU measures and analyzing them

Commission Recommendation C(2019) 2400 final
on cybersecurity in the energy sector

Real-time requirements

- *Use international standards*
- *Apply physical measures*
- *Classify/manage your assets*
- *Consider privately owned communication networks, or consider specific measures*
- *Split system 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 hard- and software*

Source: Rémi Mayet
Directorate General for Energy
Deputy Head Security of Supply
European Commission

Overview of EU measures and analyzing them

Commission Recommendation C(2019) 2400 final
on cybersecurity in the energy sector

Calls Member States to ensure that the relevant stakeholders take the necessary measures and encourage them to build up knowledge and skills related to cybersecurity in energy

It means compliance:

- NIS Directive (CSIRT, operators of essential services)
- CI legislation (list of CI)
- Cybersecurity Act (ENISA, cybersecurity certification framework for digital products, services and processes)
- Security of GAS supply regulation
- Regulation on Electricity Risk Prepardness

Overview of EU measures and analyzing them

EnC Member States relevant stakeholders must act to take the necessary legal measures to build up knowledge and skills related to cybersecurity in energy

It means have a legislation which is compatible with:

- NIS Directive (CSIRT, operators of essential services)
- CI legislation (list of CI)
- Cybersecurity Act (ENISA, cybersecurity certification framework for digital products, services and processes)
- Security of GAS supply regulation
- Regulation on Electricity Risk Prepardness

Recommedations on national level

- Clear strategy for the protection of critical energy infrastructure
- Best practices should be shared by all stakeholders (CI)
  - a) risk management programme
  - b) the main vulnerabilities of the infrastructure they manage
  - c) the threats and the solutions
- The exchange of knowledge and information among all stakeholders (common standards)
- Stakeholders ensure that the public authorities at all levels are involved, continuously informed and updated (vulnerabilities and threats)
- Stakeholdersclosely cooperate with the public authorities to increase their preparedness to eventual theats.

Recommedations on national level

- the human factor is of utmost importance in the cooperation between the public and the private sectors (information sharing)
- special purpose associations are mandatory for companies to maintain security (ENTSO-E)
- public authorities from the governmental to the local level should increase their coordination (more coherent national strategy for critical energy infrastructure protection)
- the cooperation with the private sector must be efficient;
- private and the public sectors should practice regular exercises and tests
- public and the private sectors should be ready to coordinate their efforts to allocate both human and financial resources to protect critical energy infrastructure.

EnC Level Reccommendations

- EnC member states should agree on a common definition of critical infrastructure
- Stakeholders of critical energy infrastructure should cooperate with neighboring states
- Cooperation to protect critical energy infrastructure should involve not only the stakeholders/owners of critical energy infrastructure but also governments.

EnC Level Reccommendations

- NATO members should reinforce and increase the coordination and cooperation of their activities

- It would be desirable that NATO coordinates its activities with the EU/EnC NATO members in order to avoid duplications.

How to design an action plan – Legal modeling

- Create/modify the cyber security strategy in energy sector to align with EU recommendations
- Do a detailed gap analyzis of legal framework in EU for your own country (generalized country legal gap analyzis which is done by BluePrint on behalf of EnC may be used as basics) .
- Implement CI/NIS-D legal framework (define function of CA – CERT/CSIRT, E-NRA, licencees, vendors, partners) and establish legal processes
- Implement obligatory certification and awareness measures (for all stakeholders)
- Establish/enlarge the existing CERT/CSIRT to have power handling incidents in energy sector
- Create/upgrade the legal framework for international cooperation (see EU recommendations)

How to design an action plan – operational modeling

- Create/modify CA/NRA continuous risk assessment for energy sector taken in consideration EU recommendations (methodology, real-time requirements, cascading effects, technology specific) with continuous self-improvement in focus
- Have all stakeholders assessed their risk and implement continuous risk assessment and risk management
- Deploy CSIRT capability as soon as possible (monitor, assess, react, response)
- Organize country wide PPP cooperation (ISAC) in energy
- Start/continue to educate human resource to the capability level required, provide standardized education levels for critical duties (system admins, developers, CISO etc.)
- Start/continue to have awareness programs and security tests, the results of which will be included in stakeholder/country risk assessment
- Organize international (bilateral or multirateral) information exchange for energy based risks (E-ISAC, CSIRT, ENTSO-E, EN-DSO…) – EnC in focus to be a catalyst

How to design an action plan - sample

Task : Create together on workshop a simplified action plan based on EU recommendations (20 min) with the help of the presenter

How to design an action plan - discussion

How to design an action plan - conclusions

Thank you!

Thank you!

Blueprint Energy Solutions GmbH

Presenters:
Peter Grasselli
peter.grasseli@aitsa-is.com
Szabolcs Hallai
Vienna, 11.04.2019.