"The strategic role of Regulatory Authority for Energy, (RAE) in the Energy Sector ".

Workshop in the frame of "Development of EU harmonized services for training activities in the domain of critical infrastructures".

CENTER FOR SECURITY STUDIES & JOINT RESEARCH CENTRE

Regulating the energy markets

Electricity & Natural Gas

Leontini Kaffetzaki
IT & Telecommunication Dpt.

Maria Kerkidou
Natural Gas & Oil Group

March 2017
RAE operates within the following legal framework:

- **(GR) Law 2773/1999,(Directive 96/92/EC),**
  Regulating & Monitoring the energy market.

  - Upgraded to independent administrative authority.
  - Responsible for the proper operation & liberalization of the Electricity and Gas Energy Markets.
  - In this scope RAE devices and publishes studies, act on recommendations, taking decisions and making suggestions to the national official authorities proper measures.

- **(EU) Regulation No 994/2010**
  RAE has been assigned to be the Competent Authority for the assurance of the measures’ enforcement issued by the European Regulation Security of supply of natural gas.
CORE BUSINESS

• Long-term Energy Planning.

Considering:
the existing and speculated energy inventories in national, district and international level,
the intercommunal development program of the electricity and natural gas networks,
the international energy market’s trends.

Aiming at:
the fulfillment of an undivided European internal energy market and the protection of the environment
the safety of the country’s energy supply and
the reinforcement of the competitiveness

• Monitoring the operation of all sectors of the energy market and the development of infrastructures.
  Monitoring of the energy and natural gas market. Ensuring the quality, the proper maintenance level and the reliability of the transmission and the distribution systems.

• Development of all the activities in the energy sector.
  Pricing approval of non-competitive activities
  Licensing

• Consumers’ Protection
  Regulatory Measures for the proper energy markets function
  Exemption application by third-parties service obligations
INSPIRE Directive 2007/2/EC - Discover and view spatial datasets. Transparency, Open Data & High Quality of e-Services

RAE’s Geoportal
Collaboration with the Market Stakeholders

<table>
<thead>
<tr>
<th>GR Energy Market Operators</th>
<th>Greek Power Industry</th>
<th>Government</th>
</tr>
</thead>
<tbody>
<tr>
<td>• IPTO (ADMIE) The Independent Power Transmission Operator S.A. (TSO)</td>
<td>Public Power Corporation S.A (PPC) is the biggest power producer and electricity supply company in Greece.</td>
<td>Environment Physical Planning and Public Works Ministry</td>
</tr>
<tr>
<td>• HEDNO (DEDDIE) Hellenic Electricity Distribution Network Operator S.A. (DSO)</td>
<td>DEPA Public Gas Corporation of Greece S.A.</td>
<td></td>
</tr>
<tr>
<td>• LAGIE Operator of Electricity Market.</td>
<td>RES Independent Electricity Producers</td>
<td></td>
</tr>
<tr>
<td>• DESFA Hellenic Gas Transmission System Operator S.A.</td>
<td>Alternates Power Suppliers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Energy Traders</td>
<td></td>
</tr>
</tbody>
</table>
Collaboration with National and European Institutions on energy market security

National

• Digital Policy Ministry, National CERT
• Public Order & Citizen Protection Ministry
• National Intelligence Service (EYP)
• KEMEA

European

• ACER
• CEER
• DG Energy
• ENISA
Obligations under REMIT

- Registration
- Reporting
- Data Quality & Data Sharing
- Compliance with the security data framework
- Market monitoring & Market Surveillance

New legislation to set data protection standards:

- Easier access to private data
- A right to data portability
- The “right to be forgotten”
- Reporting obligations for “data handlers” in case of data theft
- Penalties in case of severe data theft incidents

Formally adopted in April 2016

The regulation will take effect after a two-year transition period

Legislation to take effect in 2018
NIS Directive (Network Information Security & SmartGrids)

- Baseline cybersecurity obligations for:
  - operators of essential services (energy, transport, banking, financial markets, health and water supply) and
  - digital service providers (search engines, e-commerce marketplaces, cloud-computing).
- Strengthen network and information security (NIS) in the European Union
- Raise resilience of CI
- Ensure Union-wide minimum cybersecurity capabilities through audits & penalties
- Introduction of NISD-competent authorities on national and sector level
- Improve (cross-border) information sharing and collaboration through reporting

An extensive variety of EU guidelines, legislation standards and frameworks!

Lead to Uncoordinated efforts which result in a variety of heterogeneous guidelines and standards. Harmonization is often seen as the key objective.
The importance of CS in the energy sector

- Energy companies and network operators are potentially among the most attacked critical infrastructures providers. Attacks are becoming more sophisticated and frequent - intended attacks!
- Costs of a disruption of service / outage to a country’s economy
- Criticality of the energy sector to the functioning of society; Any interruption to the power grid would cause substantial chaos and cascading effects resulting in financial loss.
- Motivation behind attacks usually differs from other sectors (disruption of supply).
- The energy sector has a high potential for critical disruption through sabotage attacks.
- Smart grids and smart metering are bringing significant change to the worlds power system. Experts predict that billions of smart meters and sensors will be installed worldwide over the next ten years.

Challenges
- Different guidelines / standards, often not energy specific!
- Can be unclear governance!

Issues to consider
- What are European policymakers doing about it?
- Important new EU legislation!
- What can or should European energy NRAs do?
Daily experiences show that the threat of cyber-incidents is real!

USA ICS-CERT, received and responded 295 incidents!

- Manufacturing sector accounted for 97 of these incidents,
- Energy sector reporting 46 cyber security incidents.

37% of these incidents were examples of ‘spear-phishing’!
Recent cyber-attacks in the energy Sector

- 2015, Ukraine, attack on power grid affected **225,000** customers (disconnected).
- 2013, Austria, an ICT-incident affecting parts of the energy sector.
- 2006 Germany, and parts of continental Europe, large-scale blackouts.

Overview of the Cyber Attack on the Ukraine Power Grid

Source : [https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf]
Annex 5 – History of selected Cyber-Attacks and Incidents Year

<table>
<thead>
<tr>
<th>Country</th>
<th>Target</th>
<th>Business Sector</th>
<th>Incident Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>Bangladesh National Central Bank</td>
<td>Financial Services</td>
<td>cyber-heist - financial fraud</td>
</tr>
<tr>
<td>2016</td>
<td>Belgium AFCN Energy &amp; Utilities</td>
<td>website defacement</td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>Germany Hospital Provider Health Care</td>
<td>network disruption</td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>Austria FACC Aeronautics</td>
<td>fake president fraud – financial fraud</td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>Ukraine National Power Sector Energy &amp; Utilities</td>
<td>physical destruction of equipment</td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>UK TalkTalk Telecommunication</td>
<td>credentials and credit card details theft</td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>Germany German Parliament Public Administration</td>
<td>retrieval of information, espionage</td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>France TV5 Monde Media</td>
<td>network disruption, website defacement</td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>USA Anthem Inc. Health Care</td>
<td>medical-related data theft</td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>Japan Sony Media</td>
<td>extraction of intellectual property</td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>USA AshleyMadison.com Online Services</td>
<td>credentials and user access details theft</td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>Germany Steel Mill [no name] Heavy Industry</td>
<td>physical destruction of equipment</td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>USA J.P. Morgan Chase Financial Services</td>
<td>credit card and financial data theft</td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>USA Target Corporation Retail</td>
<td>credit card and financial data theft</td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>USA Ebay Inc. Online Services, Retail</td>
<td>credentials and credit card details theft</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>USA The Home Depot Retail</td>
<td>credit card and financial data theft</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>USA Adobe Systems Software</td>
<td>credentials and credit card details theft</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>Austria National Power Sector Energy &amp; Utilities</td>
<td>network disruption</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>USA Energy Research Company Energy &amp; Utilities</td>
<td>spear phishing - retrieval of information</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Greece Global Oil Company Energy &amp; Utilities</td>
<td>spear phishing - retrieval of information</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>Japan Sony PlayStation Network Media</td>
<td>credentials and user access details theft</td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td>Iran National Nuclear Facilities Energy &amp; Utilities</td>
<td>Stuxnet – physical destruction</td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td>Global Global Oil Companies Energy &amp; Utilities</td>
<td>Night Dragon – retrieval of information</td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td>USA Heartland Credit Union Financial Services</td>
<td>credit card and financial data theft</td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td>Georgia Governmental Facilities Public Administration</td>
<td>network disruption, website defacement</td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td>Estonia Governmental Facilities Public Administration</td>
<td>network disruption, website defacement</td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td>USA TK / T.J. Maxx Retail</td>
<td>credit card and financial data theft</td>
<td></td>
</tr>
</tbody>
</table>

Attackers are often after valuable information and intellectual property such as technology for photovoltaic research and wind turbines, or data on gas field exploration. Information such as this is of high value and can generate huge profits for attackers or their sponsors.

Many power utilities companies fear disruptive attacks the most, regardless of whether it is done by internal or external attackers.
The CS level differs substantially amongst EU Member Countries

CEER, Cybersecurity Work Stream Cybersecurity report (C16-DS-24-06) - Comparison_Table

| Issue | Austria | France | Germany | Hungary | Italy | Malta | Portugal | Slovenia | Sweden | United Kingdom | EU
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>National Level</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Planning: Does an overall national strategy on cybersecurity in the country exist?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>2. Planning: In which year was the national cybersecurity strategy first approved?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Planning: Is the existing national cybersecurity strategy covering the energy sector?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>4. Governance: Does a national agency for network and information security exist?</td>
<td>L.P.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>5. Governance: Does a national Computer Emergency Response Team (CERT) or a Computer Security Incident Response Team (CSIRT) exist?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>6. Awareness: Is there a periodic status report on the state of cybersecurity? Is it written by the CERT/CSIRT or a national agency?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Energy Sector Level</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Planning: Does a list of national critical infrastructure providers in the energy sector exist?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>8. Planning: Does a dedicated cybersecurity strategy for the energy sector exist?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>9. Assessment: Has an energy sector wide cybersecurity risk assessment been performed?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>10. Governance: Does a binding national law for providers of critical infrastructure in the energy sector exist which defines which measures need to be taken for which risk level (i.e. baseline security standards)?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>11. Information Sharing: Are there providers of critical infrastructure in the energy sector obliged to report critical cybersecurity incidents? If yes to whom?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>12. Information Sharing: Does a dedicated sector-specific energy CERT/CSIRT or critical infrastructure CERT covering the energy sector exist?</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

Substantial differences in:

- Governance and Planning
- Information Sharing and Incident
- Awareness Building, Trainings
- Initiatives, Sector Exercises, PPPs
- Reporting, CERTs / CSIRTS
- Vulnerability Identification
- Risk Assessment
- Audit Processes
- Availability of (binding) baseline, Security Standards and Obligations
Initiatives for Cybersecurity in the energy sector

EU institutions, member states and private sector

• 2013, European Commission released the **Cybersecurity Strategy of the European Union**.

• **Priorities**
  1. Achieving cyber-resilience,
  2. Drastically reducing cyber-crime,
  3. Developing cyber-defence policies,
  4. Developing the industrial and technological resources for cybersecurity.

GR government and market

• 2017, Greece recently enacted the National Information Security Strategy.

• RAE is taking active part in the efforts made by the Hellenic Environment Physical Planning and Public Works Ministry, the Hellenic Ministry of Digital Policy Cybersecurity and the Greek National Centre for Security Studies (KEMEA) to build Cyber security awareness and the implementation of standardized security policies, among the stakeholders in energy sector.
Actions for European energy NRAs to consider

• **Clearly define** the desired NRA role, engagement level and strategy.

• Identification of Operators of Essential Services.

• Better understand vulnerabilities and the risk landscape.

• Encourage and support energy sector-specific quantitative risk assessments.

• Support *information-sharing initiatives and collaboration* between public and private stakeholders and institutions at EU and National level.

• Drive CS-awareness and introduce *simple and clear baseline security and safety standards*. 
Regulation (EU) No 994/2010
Concerning measures to safeguard security of gas supply

• Aims at demonstrating all necessary measures are being taken to ensure continuous supply,
  • in case of difficult climatic conditions
  • in the event of disruption

  • established the Gas Coordination Group

• Gas Coordination Group
  • a platform to exchange information between MSs, the Commission, the gas industry and consumers.
Regulation (EU) No 994/2010, 
Provisions aimed at safeguarding the security of gas supply

- Designation of the "Competent Authority’ by each Member State to be responsible for ensuring the implementation of the measures set out in this Regulation

  ➢ RAE has been designated as the Competent Authority, (article 12 L.4001/2011 ,FEK A’ 179, 22.08.2011)

- Elaboration of Risk Assessment

Regulation (EU) No 994/2010,
Provisions aimed at safeguarding the security of gas supply

- Ensuring, in the event of a disruption of the single largest gas infrastructure, the capacity of the remaining infrastructure, determined according to the N – 1 formula, is able to satisfy total gas demand of the calculated area during a day of exceptionally high gas demand occurring with a statistical probability of once in 20 years. (infrastructure standard)

- Ensuring of gas supply to the protected customers of the Member State in the following cases: (supply standard)
  
(a) extreme temperatures during a 7-day peak period occurring with a statistical probability of once in 20 years;

(b) any period of at least 30 days of exceptionally high gas demand, occurring with a statistical probability of once in 20 years; and

(c) for a period of at least 30 days in case of the disruption of the single largest gas infrastructure under average winter conditions
Risk Preparedness
updated every 2 years, notify the Commission

• Risk assessment
  a full assessment of the risks affecting the security of gas supply
  Shall be updated every 2 years unless circumstances warrant more frequent updates.

• Preventive Action Plan (RAE’s decision 429/2015)
  establish a list of predefined actions to make gas available in the event of an emergency
  Consultation between Competent Authorities of neighboring countries

• Emergency Plan (RAE’s decision 405/2015)
  establish detailed procedures and measures to be followed for each crisis level,
  define the role and responsibilities of the natural gas undertakings

In order to allow the internal gas market to function even in the face of a shortage of supply, it is necessary to provide for solidarity and coordination in the response to supply crises
In energy “cyber” security, the primary goal is to ensure security of supply!
Thank you for your attention!

Contact
leontini@rae.gr  mkerkidou@rae.gr

Regulatory Authority for Energy
132 Piraeus Av., 11854, Athens, Greece
Tel: +30 (210) 37 27 400
e-mail: info@rae.gr
url: www.rae.gr