Comparison of Nordic and Continental Europe Grids from the Cyber Resilience Perspective

Dr. Hayretdin Bahşi
Tallinn University of Technology
Centre for Digital Forensics and Cyber Security
Main Aim

• Cyber resiliency comparison
  o Nordic Grid
  o Continental Europe Grid

• Recommendations for
  o Descynchronization from IPS/UPS
  o Synchronization with Nordic or Continental Europe
Synchronisation

• Exchange of real-system data for frequency balancing
  o Between SCADAs of Baltic Region and Russia
  o Inter-control Centre Communications Protocol on TCP/IP
  o Both sides run server and client modules
  o Bidirectional data exchange

• Attack surface
  o No hierarchical relationship between SCADAs
  o No access right on the other SCADA
  o Dedicated network lines
Cross-border Dependency

• Dependency types
  o Physical, cyber, geographic and logical

• Cyber dependency
  o Exchange of local system data
  o Intervention of operators in case of problem

• Physical dependency
  o Frequence balancing function
<table>
<thead>
<tr>
<th>Level</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| **Grid Level**                | • Global Cyber Security Index (Legal, Technical, Organizational, Capacity, Cooperation)  
                              | • Grid Level Information Sharing and Incident Handling                        |
| **National Level**            | • Global Cyber Security Index (Legal, Technical, Organisational, Capacity Building and Cooperation) |
| **Critical Infrastructure Level** | • CI Level Regulatory Framework  
                              | • CI Level Incident Handling  
                              | • CI Level Crisis Management  
                              | • Cooperation with R&D Organisations |
| **Energy Sector Level**       | • Sector Level Regulatory Framework  
                              | • Sector Level Incident Handling  
                              | • Sector Level Crisis Management |
| **Transmission System Operator Level** | • Information Security Management Framework  
                              | • Business Continuity Framework |
Baseline of Comparison
Out of Scope Issues

• Analysis of specific cyber risks of transmission systems
  o Due to the confidentiality requirements

• Strategic analysis of cyber threats
  o Motivation of cyber threat actors
  o Investments of cyber threat actors for cyber security operations
Method

• Desk review of
  o National cyber security strategies
  o Analysis reports of organisations such as
     European Union Agency for Network and Information Security (ENISA)
     Energy Expert Cyber Security Platform
  o Open information sources about the activities of TSOs

• Surveys and interviews
  o Elering AS and Fingrid Oyj completed the survey
  o PSE rejected answering the survey due to the confidentiality concerns
Data Sources for National Level Comparison

• Global Cybersecurity Index 2014 and 2017
  o Conducted by International Telecommunication Union (ITU)
  o Evaluation against five pillars
    • Legal, technical, organisational, capacity building and cooperation
  o Categories of countries: leading, maturing and initiating

• Wide-scale analysis of Internet
  o Non-profit organisation, Cyber Green Institute
  o Misconfigured DNS, NTP, SNMP, SSDP services and Mirai infections
  o DDoS amplification attack vectors
  o Country-based results
Data Sources for National Level Comparison (2)

• Microsoft security intelligence reports
  o Country-based results
  o Quarterly reports
  o Security metrics
    • Malware encounter rate
    • Drive-by-download web pages
    • Phishing sites
    • Malware hosting web-sites
Changes in Energy Ecosystem

• Efficiency and de-carbonisation aims of energy policy
  o Distributed energy resources and two-way energy flow
  o Increased dependence on IT systems via Smart Grids

• More integration of business and operational processes
  o More integration of ICT (information and communication technology) and OT (Operational Technology) systems
  o Sophistication levels of cyber threat actors
Overview of Cyber Resiliency of Critical Infrastructures

  o Adopted on 6 July 2016

• Lack of frameworks in energy sector

• Maturity level assessment of ICS-SCADA cyber security by ENISA
  o Leaders, who have the highest maturity level, are not mature enough in some subjects

• Integration of cyber resilience into the overall resilience

• EU, as a whole, is in a developing stage.
# TSO Level Comparison

<table>
<thead>
<tr>
<th>Polish TSO (PSE S.A)</th>
<th>Finnish TSO (Fingrid Oyj)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formal conformity to information security and business continuity management standards</td>
<td>Uses information security management standard, ISO 27001, as a framework</td>
</tr>
<tr>
<td></td>
<td>Continuity management project was completed in 2014</td>
</tr>
<tr>
<td>Has a CERT Team</td>
<td>No specific CERT Team</td>
</tr>
<tr>
<td>No information about the cyber exercise capabilities</td>
<td>Cooperation with JYVSECTEC in creating cyber ranges for critical infrastructure protection</td>
</tr>
<tr>
<td></td>
<td>Operational level crisis management exercises include cyber security</td>
</tr>
</tbody>
</table>
## Critical Infrastructure and Energy Level Comparison

<table>
<thead>
<tr>
<th>Poland</th>
<th>Finland</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has a critical infrastructure protection program but the link with actual cyber resilience activities is missing</td>
<td>Implementation Programme for Finland’s Cyber Security Strategy for 2017–2020 has specific item for the protection of electricity sector. Specific budget and human resources are assigned to National Emergency Supply Agency (NESA).</td>
</tr>
<tr>
<td>Cybersecurity Foundation organizes cyber security exercises for critical sectors (2012 for energy companies)</td>
<td>Conducts cyber security exercise in each year in the facilities of JYVSECTEC. Fingrid Oyj, with Elenia Oy, started to conduct cyber exercise for the sector operators in 2017.</td>
</tr>
<tr>
<td>Cooperation with a R&amp;D institution has not been identified</td>
<td>VTT Technical Research Centre is in cooperation with NESA conducts several cyber security projects including industrial control system security.</td>
</tr>
<tr>
<td>Any regulation for electricity transmission sector has not been identified.</td>
<td>Any regulation for electricity transmission sector has not been identified.</td>
</tr>
</tbody>
</table>
Critical Infrastructure and Energy Level Comparison (2)

- Both countries have not developed mature national capabilities
- Minor superiority of Finland over Poland in this comparison item
  - Solid responsibilities and action items in Finnish Implementation Program
  - Additional systems that run by Finnish CSIRT
  - Cooperation with R&D institutions in industrial control system security area
National Level Comparison – Cyber Security Commitments

- Global Cybersecurity Index studies (in 2014 and 2017)
  - In 2017 study, Finland is ranked as 16, Poland as 33
  - In 2014 study, 22 states have higher score than Finland and 35 states are better than Poland
  - Finland is better than Poland in both studies
Cyber Green Institute Data

Poland: 21 million IP addresses
Finland: 13 million IP addresses
Microsoft Security Intelligence Reports

<table>
<thead>
<tr>
<th>Security Metric</th>
<th>Poland (1Q17)</th>
<th>Finland (1Q17)</th>
<th>World Average (1Q17)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encounter Rate</td>
<td>7.7</td>
<td>2.9</td>
<td>9.06</td>
</tr>
<tr>
<td>Drive-by download pages</td>
<td>0.10</td>
<td>0.09</td>
<td>0.17</td>
</tr>
<tr>
<td>Phishing Sites</td>
<td>7.3</td>
<td>2.4</td>
<td>6.3</td>
</tr>
<tr>
<td>Malware Hosting Sites</td>
<td>6.1</td>
<td>4.1</td>
<td>14.8</td>
</tr>
</tbody>
</table>
Comparison of TSO, Energy and Critical Infrastructure Levels

• No major difference between TSOs, Svenska Kraftnät and 50Hertz

• Sweden
  o Detailed guidance about information security management
  o National contingency authority is responsible for implementation of cyber security strategy

• Germany
  o Strong information security authority which has advanced technical and organisational capabilities
  o Strong legal framework with IT Security Act
National Level Comparison

- Global Cyber Security Index
  - In 2017, Germany → 24, Sweden → 17
  - In 2014, Germany → 8, Sweden → 20

<table>
<thead>
<tr>
<th>Security Metric</th>
<th>Germany (1Q17)</th>
<th>Sweden (1Q17)</th>
<th>World Average (1Q17)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encounter Rate</td>
<td>4.26</td>
<td>3.5</td>
<td>9.06</td>
</tr>
<tr>
<td>Drive-by download pages</td>
<td>0.03</td>
<td>0.03</td>
<td>0.17</td>
</tr>
<tr>
<td>Phishing Sites</td>
<td>5.1</td>
<td>3.3</td>
<td>6.3</td>
</tr>
<tr>
<td>Malware Hosting Sites</td>
<td>7.0</td>
<td>5.7</td>
<td>14.8</td>
</tr>
</tbody>
</table>
Cyber Green Institute Data

Germany: 120 million IP addresses

Sweden: 27 million IP addresses
Grid Level Comparison

• According to Global Cybersecurity Index 2017
  o Distribution of 24 members of Continental Europe Synchronous Area: 20 maturing, 3 leading and 1 initiating
  o Members of Nordic Synchronous Area: Finland, Sweden and Norway are leading states. Denmark, as being the member of both grids, belongs to the maturing category.

• States that have specific Energy or Critical Infrastructure CERT
  o KraftCERT in Norway
  o CERTSI in Spain
Grid Level Comparison (2)

• Nordic Region Cooperation
  o Nordic National CERT Collaboration between Norway, Sweden, Iceland, Finland and Denmark
  o Cross-country cooperation platform created by Nordic banks, Nordic Financial CERT
  o High level regional cooperation framework, Nordic-Baltic Eight (NB8)
    o Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway and Sweden
    o Energy and Cyber security are among the agenda items
  o A table top exercise regarding an energy shortage scenario in the region in October 2014
## Overall Results (Finland vs Poland)

<table>
<thead>
<tr>
<th>Overall Comparison</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TSO Level Comparison</strong></td>
<td>• No any significant differences between the cyber resilience levels of Finnish and Polish TSOs</td>
</tr>
</tbody>
</table>
| **Energy and Critical Infrastructure Level Comparison** | • The limited reflection of national programs to the energy sector in general and electricity transmission sector, in particular  
• Involvement of more players such as emergency management authority and R&D organisations in Finland |
| **National Level Comparison** | • Finland has a better position in Global Cyber Security Index 2017  
• Finland is better according to the data of Cyber Green Institute and Microsoft Security Intelligence Reports |
# Overall Results (Germany vs Sweden)

<table>
<thead>
<tr>
<th>Overall Comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TSO Level Comparison</strong></td>
</tr>
</tbody>
</table>
| **Energy and Critical Infrastructure Level Comparison** | • Guidance-based approach (Sweden) vs regulation-based approach (Germany)  
• Better crisis management capability (Sweden) vs strong information security authority (Germany) |
| **National Level Comparison** | • Germany has a better position in Global Cyber Security Index 2014, Sweden has better score in 2017 study  
• Germany is better than Sweden in some metrics of Cyber Green Institute  
• Sweden has lower ratios in some categories according to Microsoft Security Intelligence Reports |
Overall Results (Grid-Level Comparison)

• The rankings of Nordic Grid Members are higher than the Continental Europe Grid Members in Global Cybersecurity Index 2017

• The national CERTs belonging to both grids are indistinguishable in terms of their contribution to critical infrastructure protection

• There exists a collaboration culture between Nordic countries. However, the contribution to cyber resilience in energy systems is limited
  o Solid operational framework does not exist
  o The size of the information sharing network is low
Conclusion

• Finland vs Poland
  o Finland is better in national level comparison
  o They need to improve themselves in critical infrastructure and energy levels

• Germany vs Sweden
  o No major difference

• Nordic Grid has better Global Index average
Conclusion (2)

This study concludes with some caveats, that Nordic Grid is a better option for the Baltic States from the cyber resilience perspective.