CYBER SECURITY OF SMART GRID - CHALLENGES AND POTENTIAL SOLUTIONS FOR TRANSMISSION SYSTEM OPERATORS

Mihai PAUN
Vice-President
Romanian Energy Center

SUCCESS Project

First Innovation Event

CYBER SECURITY FOR SMART GRID

22/09/16 Terni, Italy

CRE
Romanian Energy Center

success
securing critical
energy infrastructures

CONTENT

- Romanian Energy Center (CRE) – Objectives & Activities
- Cyber Security of Smart Grid - Securing Critical Energy Infrastructures
  - Risk assessment
  - Cyber Security Incidents
  - Cyberterrorist Threats to Power Grid
- EU Projects with CRE's participation
  - The Role of CRE in SUCCESS Project
- Possible Solutions and Recommendations

CRE
Romanian Energy Center

Romanian Energy Center - CRE

- The Romanian Energy Center is a non-governamental and non profit Association representing the interest of state-owned and private companies operating in the Romanian Energy Market, in relation with EU and National Institutions;

- CRE contributes to European decision-making with the aim of encouraging and promoting investments in low-carbon technologies and support the transition to a decarbonized energy system.

CRE
Romanian Energy Center

MEMBERS - CRE

15 Members: public and private sector

- ADREM INVEST
- BIOENERGY
- CEZ România
- Complexul Energetic Oltenia
- ELECTRICA
- ECRO
- E.ON România
- ENERGOBIT
- EXIMPROD
- INSTITUTUL DE STUDII SI PROIECTARI ENERGETICE
- ROMGAZ
- TRACTEBEL ENGENEERING – GDF SUEZ
- TRANSELECTRICA
- TRANSGAZ
- ŢUCA ZBARCEA & ASSOCIATES

Romanian Energy Center - CRE

- Events in Romania and Brussels
- Position papers to Romanian and European policy consultations
- Coordinator of the Center for Dialogue and Cooperation 16+1 – China CEEC

ROMANIA ENERGY DAY 2016

"Regional and European Values for Sustainable Energy in Central and Eastern Europe"

5th Romanian ENERGY DAY, Bruxelles

- **OBJECTIVE** – **To Inform** the representatives of EU institutions in Bruxelles and to contribute to EU decision making process regarding energy priorities, projects and programs in Central and South-East Europe and in Romania;

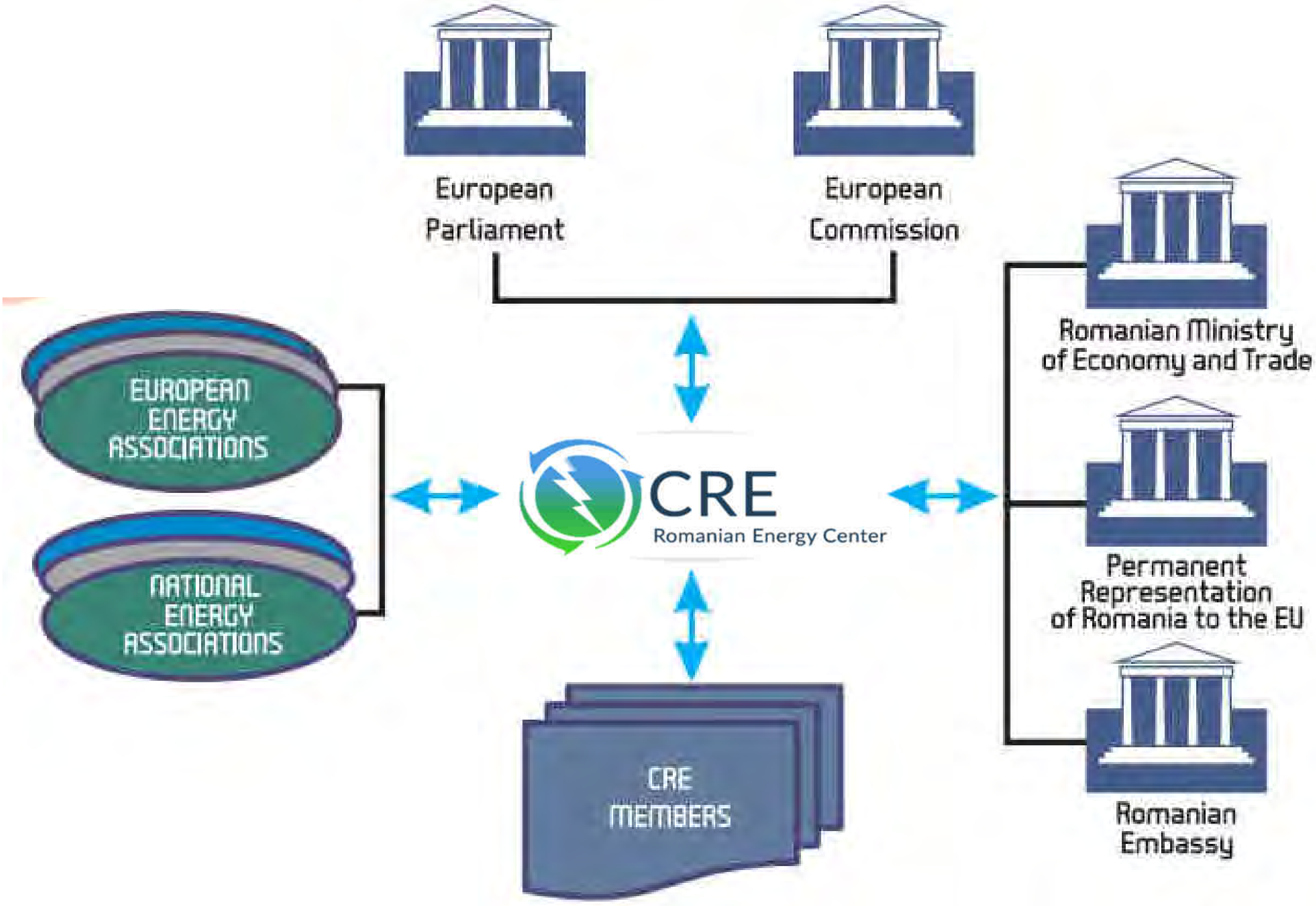
– **To Facilitate investments in energy infrastructure, to support Energy Market Integration and to increase energy security in the Region;**

– **To proactively contribute to the development of HV electricity, oil and gas corridors and to increase interconnection capacity in the Region**;

- **Media coverage** – Euractiv, Calea Europeana, Radio România Actualităţi, TVR, Mondonews.ro, Energynomics.ro, Libertatea.ro, Digi24, www.stiripesurse.ro

CRE
Romanian Energy Center

Romanian Energy Center - CRE


European Parliament
European Commission
EUROPEAN ENERGY ASSOCIATIONS
NATIONAL ENERGY ASSOCIATIONS
CRE
Romanian Energy Center
Romanian Ministry of Economy and Trade
Permanent Representation of Romania to the EU
Romanian Embassy
CRE MEMBERS

CRE
Romanian Energy Center

CRE
Romanian Energy Center

Consolidating the European dimension of the Romanian Power Sector

CRE Bucuresti
Str. Sofia, nr. 6, etaj 1,Sector 1, Bucuresti, România 011838
Tel +4 021 7953020; +4 0723 735 140
Fax +4 021 7953020
office@crenerg.org / www.crenerg.org

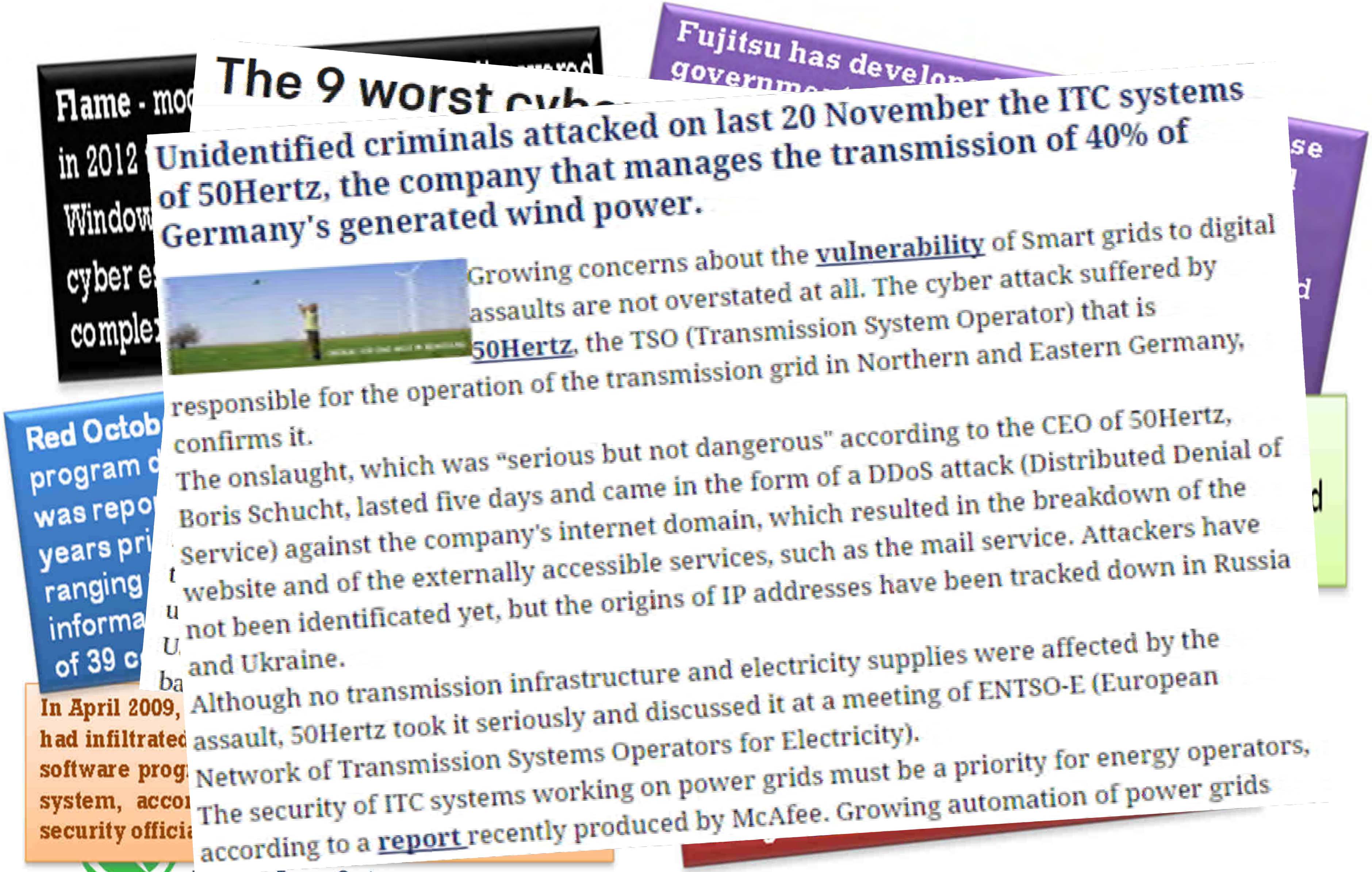
CRE Bruxelles
Bruxelles - Romanian Energy Center - CRE
Rue Montoyer 23, B-1000, Brussels, Belgium
Tel: +4 021 7953020
office@crenerg.org / www.crenerg.org

CYBER SECURITY OF SMART GRID

Securing Critical Energy Infrastructures

CRE
Romanian Energy Center

USUAL DAILY NEWS ON INT'L MEDIA



Flame - mo
in 2012
Window
cyber e
comple

The 9 worst cyb

Fujitsu has develo
governme
se
d

Red Octob
program o
was repo
years pri
ranging
informa
of 39 c

t
u
U
ba

In April 2009,
had infiltrated
software prog
system, accor
security offici

Unidentified criminals attacked on last 20 November the ITC systems of 50Hertz, the company that manages the transmission of 40% of Germany's generated wind power.

Growing concerns about the **vulnerability** of Smart grids to digital assaults are not overstated at all. The cyber attack suffered by **50Hertz**, the TSO (Transmission System Operator) that is responsible for the operation of the transmission grid in Northern and Eastern Germany, confirms it.

The onslaught, which was "serious but not dangerous" according to the CEO of 50Hertz, Boris Schucht, lasted five days and came in the form of a DDoS attack (Distributed Denial of Service) against the company's internet domain, which resulted in the breakdown of the website and of the externally accessible services, such as the mail service. Attackers have not been identified yet, but the origins of IP addresses have been tracked down in Russia and Ukraine.

Although no transmission infrastructure and electricity supplies were affected by the assault, 50Hertz took it seriously and discussed it at a meeting of ENTSO-E (European Network of Transmission Systems Operators for Electricity).

The security of ITC systems working on power grids must be a priority for energy operators, according to a **report** recently produced by McAfee. Growing automation of power grids

Romanian Energy Center

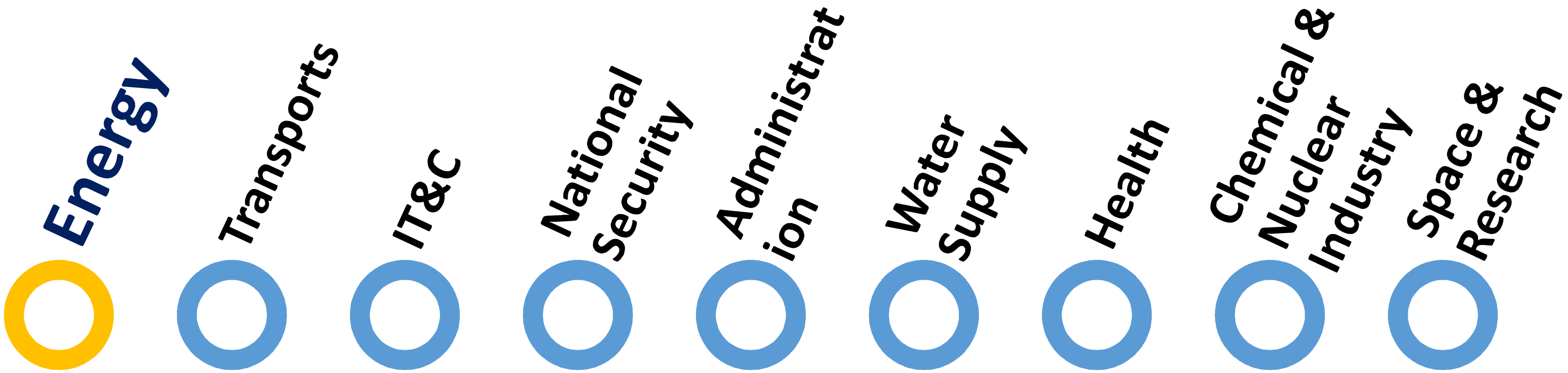
EXAMPLES OF CRITICAL INFRASTRUCTURE TARGETED BY CYBER TERRORISM

- Electricity, Gas & Oil Grids
- Finance & Banking
- Passengers Transportation
- Human health
- Agricultural health
- ICT Systems & Infrastructure
- Cities & Major Civil Works

NEED FOR STRENGTHENING EU ACTIONS AGAINST CYBER TERRORIST THREATS

CRE
Romanian Energy Center

ROMANIAN CRITICAL INFRASTRUCTURES



Energy

Transports

IT&C

National Security

Administration

Water Supply

Health

Chemical & Nuclear Industry

Space & Research

MINISTRY OF INTERNAL AFFAIRS

Centre for Coordination of Critical Infrastructure Protection

CRE

Romanian Energy Center

CYBERTERRORIST THREATS TO POWER GRID

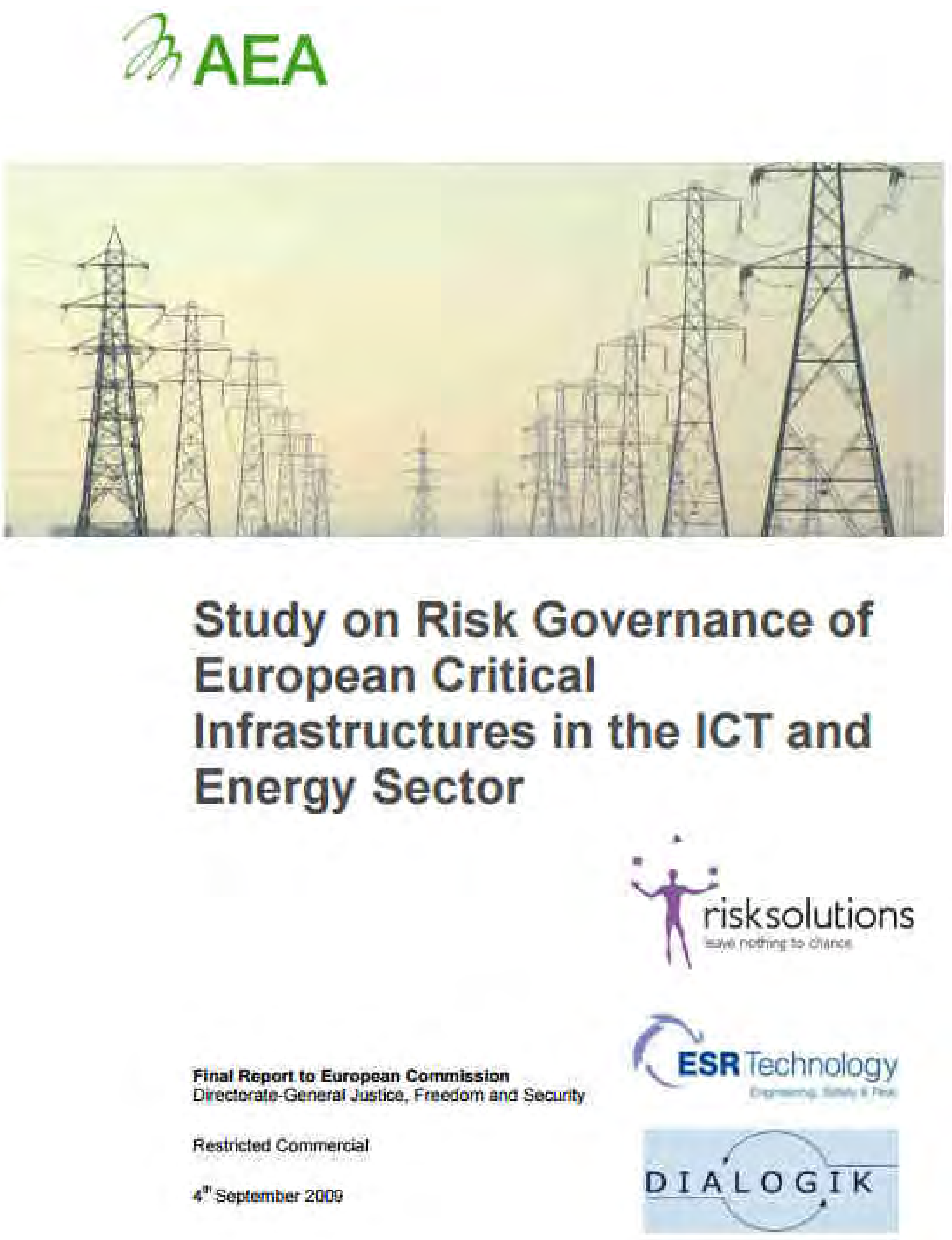
- Threats to critical infrastructure
- Threats to Networked Control Systems
- Direct – Action Threats to Power Grid
- Threats to Trustworthy Cyber-Infrastructure for Power (TCIP)

Which is more critical, the power grid, its nodes or the human resource?

CRE
Romanian Energy Center

RISK ASSESSMENTS

- Several experts → DSOs, and maybe also TSOs, should conduct mandatory risk assessments
- Critical assets and processes → to be identified
- The most critical threats (e.g. intentional threats) → to be identified
- Define a Plan to address them
- Mandatory risk assessments should be based on a selected methodology



AEA

Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector

Final Report to European Commission
Directorate-General Justice, Freedom and Security

Restricted Commercial

4th September 2009

risksolutions

ESR Technology

DIALOGIK

CRE
Romanian Energy Center

CYBER SECURITY INCIDENTS

- A cyber security incident can impact any domain along the value chain
- Stakeholders will have to be involved depending on the type of incident
- From electricity generators to consumers, and
- At all levels, from infrastructures to services and operations
- Pay attention to value-chain interdependencies, as for example among DSOs, with TSOs, retailers, etc.
- Impact on other critical infrastructures at the national and European levels.

INCIDENT DETECTION

- TSOs and DSOs are in charge of incident detection
- TSOs and DSOs need to perform monitoring actions to detect possible incidents affecting the European power grid as a whole and also in each MS.
- In European-wide incidents → TSOs should be the organisations in charge of monitoring and triggering alarms.
- Experts mentioned the IRRIS FP7 IP Project as a reference for the creation of an alarming system for grid operators.

Technical aspects of cyber security Incident detection

- Security monitoring sensors → distributed across the grid & gathering data that could be processed in a decentralised or centralised manner;
- A Central Monitoring Centre for data collection and analysis could adopt the structure of a Security Operations Centre (SOC); → Regional Cooperation Centers
- Signature-based software will be needed in sensors
- Correlation & intelligence capabilities can be distributed acros r included in the SOC;
- Intelligence → able to distinguish if the root caus a cyber security event or any other event;
- Monitoring Centres could also perform r es (i.e. write new signatures, study new threats, etc.).

+
THE HUMAN RESOURCE

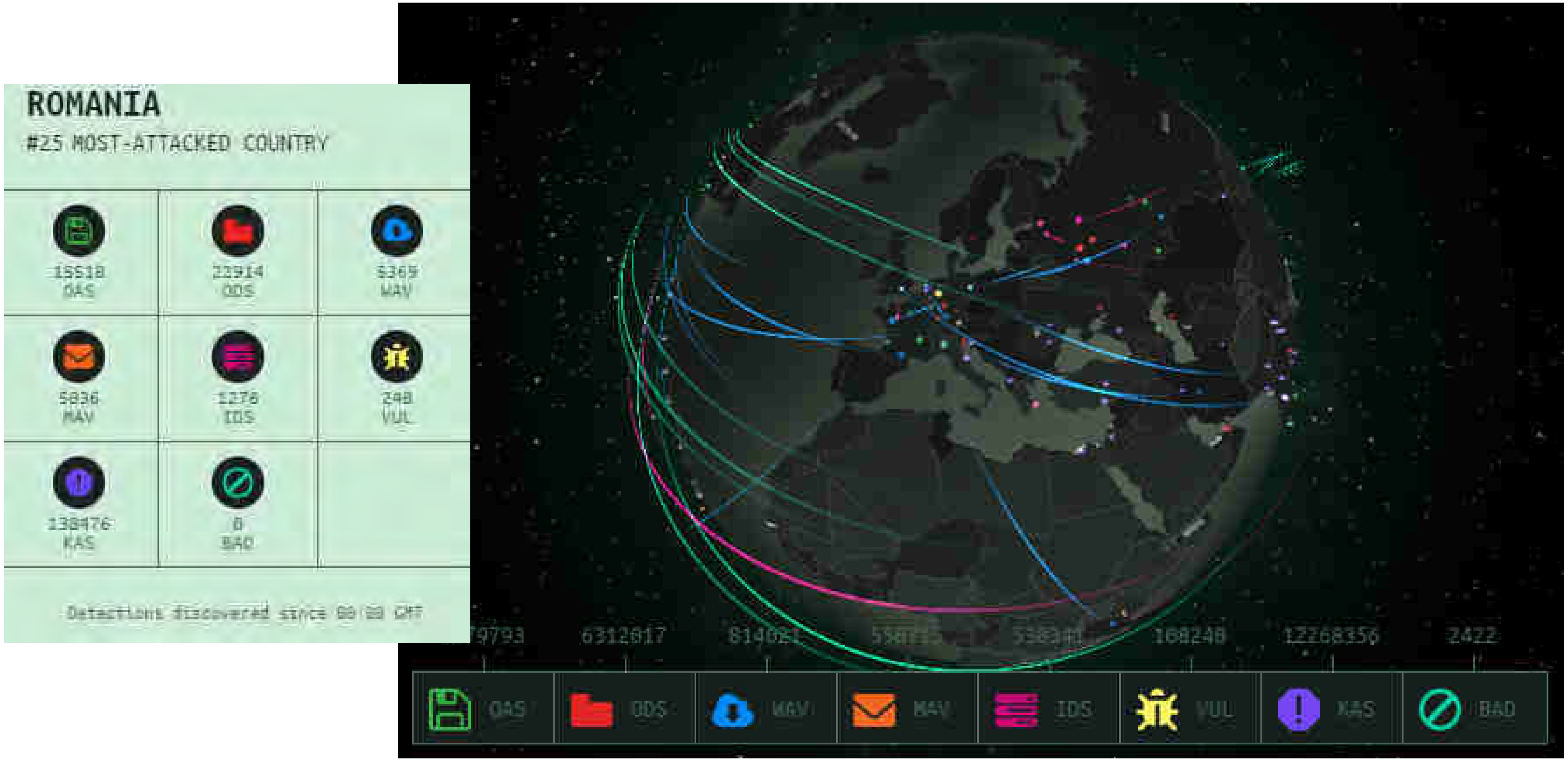
CRE
Romanian Energy Center

MANAGING INCIDENTS

- A cyber security incident can impact any domain along the value chain
- TSOs and DSOs → experience with incidents of different type (e.g. blowing of transformers due to an overload).
- There are structures and mechanisms in place, at the organisational and coordination level and also at the technical level that should be considered (e.g. for TSOs Cooperation: CORESO – Brussels + TSC – Munich)
- TSOs and DSOs → experience in restoring the power service

CRE
Romanian Energy Center

CYBERTHREAT REAL-TIME MAP



ROMANIA

#25 MOST-ATTACKED COUNTRY

15518 OAS	22914 ODS	5369 WAV
5836 MAV	1276 IDS	248 VUL
138476 KAS	0 BAD	

Detections discovered since 00:00 GMT

https://cybermap.kaspersky.com/

success

securing critical
energy infrastructures

SUCCESS - Securing Critical Energy Infrastructures

CRE
Romanian Energy Center

CURRENT INVOLVMENT OF CRE IN EU PROJECTS
RE-SERVE, SUCCESS, WiseGRID

Renewables in a Stable Electric Grid

SUCCESS - Securing Critical Energy Infrastructures

Wide scale demonstration of Integrated Solutions and business models for European smart GRID success

securing critical
energy infrastructures

- **SUCCESS - Securing Critical Energy Infrastructures**
- Work programme objective addressed: **H2020-DRS-2015**
- Topic addressed: **DRS-12-2015**
- Topic (1): **Critical Infrastructure “smart grid” protection and resilience under “smart meters” threats**
- **Research and Innovation Action (RIA)**

The Role of the Romanian Energy Center - CRE in SUCCESS Project

- **WP3 → Securing Smart Devices**
- **WP4 → Securing Smart Infrastructure**
  - **Task 4.3 - Pan-European Security Monitoring Centre**
- **WP5 → Demonstrations, field trials and evaluations of Solutions for Secure Solutions for Smart Metering**
  - **Task 5.2: Romanian Trial (Leader: ELECTRIC, Participant: CRE)**

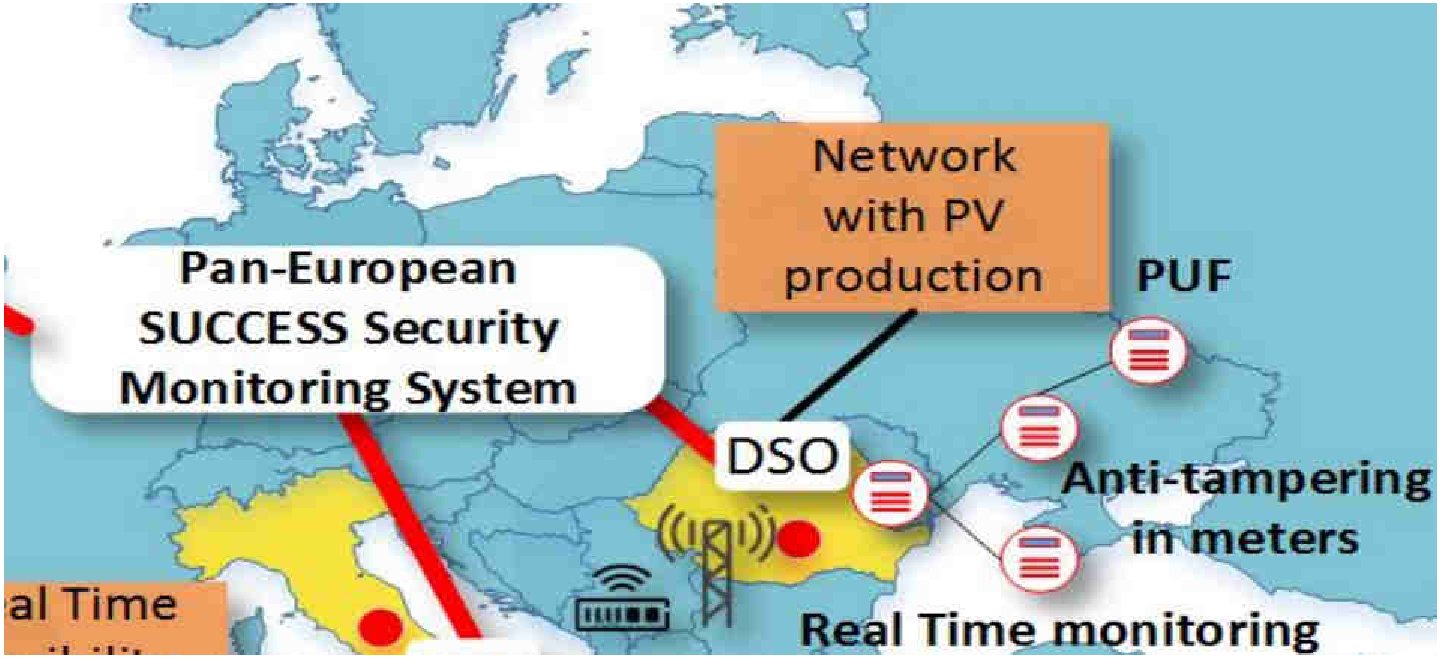
- **TOTAL: 28 pm**

CRE
Romanian Energy Center

The Role of ELECTRICA in SUCCESS Project
ELECTRICA demo site

Site: 5-10 metering points in an MV network with massive renewables production (PV, maybe also wind) DSO network with temporary power injection from MV back in HV network

Testing: Real-time monitoring using 5-10 NORMs
Assessment of low cost PMU part of NORM
PUF related tests


Network with PV production
PUF
Pan-European SUCCESS Security Monitoring System
DSO
Anti-tampering in meters
al Time
Real Time monitoring

CRE
Romanian Energy Center

POSSIBLE SOLUTIONS AND RECOMMENDATIONS

- The European Commission (EC) and the Member States' (MS) competent authorities should undertake initiatives to improve the regulatory and policy framework on smart grid cyber security at national and EU level
- Public-Private Partnership (PPP) could be created to coordinate smart grid cyber security initiatives
- Foster awareness raising, training, dissemination and knowledge sharing initiatives
- Develop a minimum set of security measures based on existing standards and guidelines
- Further study and refine strategies to coordinate measures countering large scale pan-European cyber incidents affecting power grids.
- CAPACITY BUILDING AT INSTITUTIONAL LEVEL!

CRE
Romanian Energy Center

Source: Smart Grid Security - ENISA

THANK YOU!

Dr. Mihai PAUN
Vice-President
Romanian Energy Center
37 Square de Meeûs, 4th Floor, 1000 Brussels, Belgium
+3227917531; +32478652803
Mihai.Paun@crenerg.org
www.crenerg.org

CRE
Romanian Energy Center