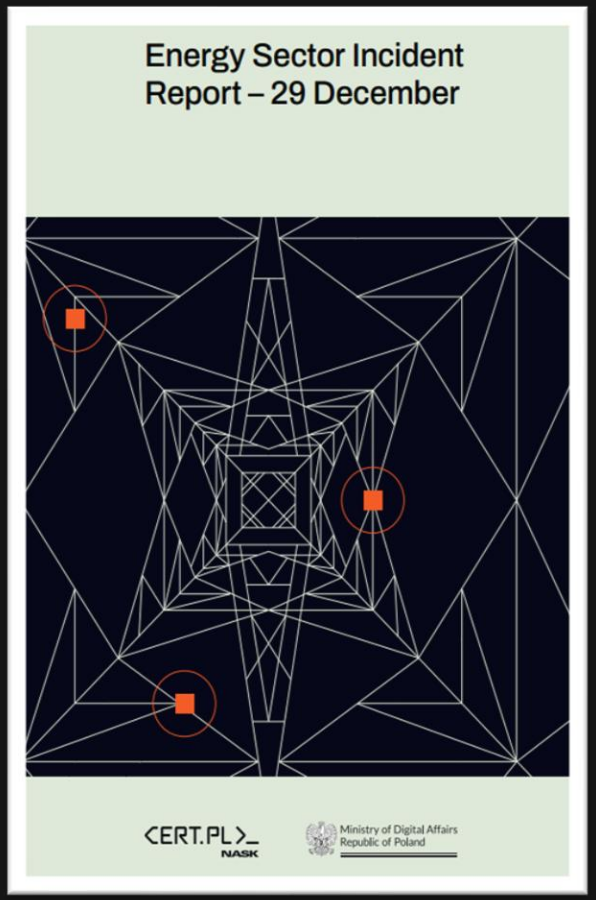
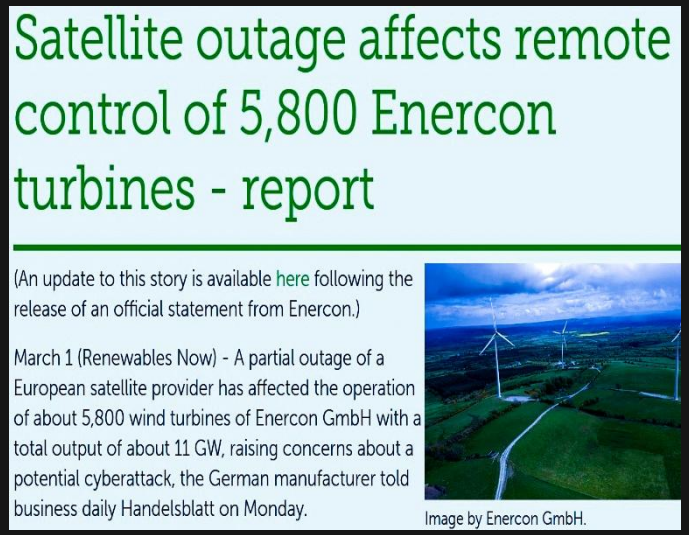
Cybersecurity Dimension of Critical [Energy] Infrastructure Protection





Views expressed in this presentation are the authors' and do not represent the official view of any institution he is affiliated with.

Roundtable on ENSEC in SEE
(Panel D) European Parliament
19 March 2026 17:45

Vytautas Butrimas
Industrial cybersecurity consulting
Voting Member ISA 99
PERA+ participant
Moderator SCADASEC
vyto2b@hotmail.com

We are still struggling in critical energy infrastructure protection

We continue to fail in determining

- What needs to be protected
- From what threats
- How to protect identified assets from identified threats

This has led to bad policy and increasingly serious incidents

- NIS2/CRA data centric, vague definitions - “devices with digital elements”, not about systems
- Iberian peninsula blackout April 2025 (inverters not allowed)
- December 29th cyber attack on renewable energy control infrastructure. (Operator use of defaults, did not apply sec)

Very poor answers in Europe as well

What to protect – “products with digital elements”

Threats - ransomware and cybercrime

Measures - similar to IoT (smart speakers)

Missing: awareness of APT threats and devices they are targeting in C.I.

CRA – 100 pages, CRA Draft “Guide” – 70 pages !

Failure to answer the 3 security questions is turning out bad policy

Curious national strategy document to specifically list a baby monitor and fitness device for protective measures, yet no mention of the ubiquitous PLC. Sounds like the drafters are distracted by infants at home and keeping slim.

Protecting Baby Monitors or PLC's? Impressions of the U.S. National Cybersecurity Strategy of 2023

Edit article View stats

Vytautas (Vytas) Butrimas
Industrial cybersecurity Consultant, Performed Cyber Risk Study of the ICS used in the NATO CEPS.

5 articles

March 15, 2023

Like Comment Share 11

http://scadamag.infracritical.com/index.php/2023/03/15/impressions-of-the-u-s-national-cybersecurity-strategy-of-2023/

Other problems in policy making and implementation

Government level,

- Many decision makers have no idea about industrialcontrol system (ICS) “OT” environments, but they are getting lots of input from IT consultants and suppliers

Government gets almost no input from the ICS/ACS/OT world.

- Standards organizations and others are trying to inform BUT …..

Conflicting guidance from ISA, ISO, NIST, NAMUR, etc.,

- each industry has its own terminology and special requirements

First of all, operationally, "Its more Complicated"

Further driven by climate change

Managing interconnected grids, **high renewable penetration**

- voltage stability
- reactive power balance
- protection coordination

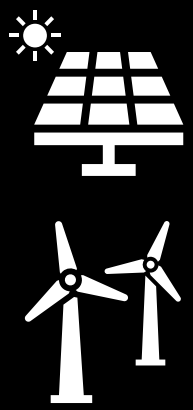
Need for heightened scrutiny

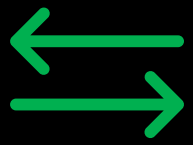
- record-high connection queues
- surging data center demand
- unparalleled stress on transmission infrastructure worldwide.

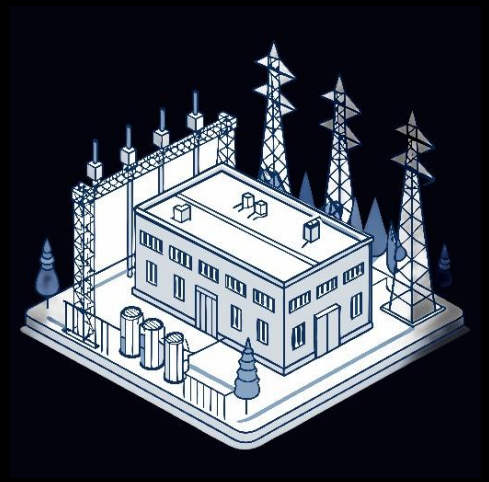
Malicious Cyber Activities of States

Cyber attack on Polish Power Grid 29 December 2025

- Attacker gained access via Internet facing devices
- Disabled communication devices, “bricked RTU’s”, wiped data
- Over 30 substations, Heating plant, manufacturing site
- DSO lost view and control, but power flowed normally
- Devices were in “default” configurations, security features disabled







DSO

Wind farm and Substation images from https://stock.adobe.com/lt *No signal* from https://commons.wikimedia.org/wiki/File:No_Signal_23.JPG

Are we falling into Cyberg thinking?

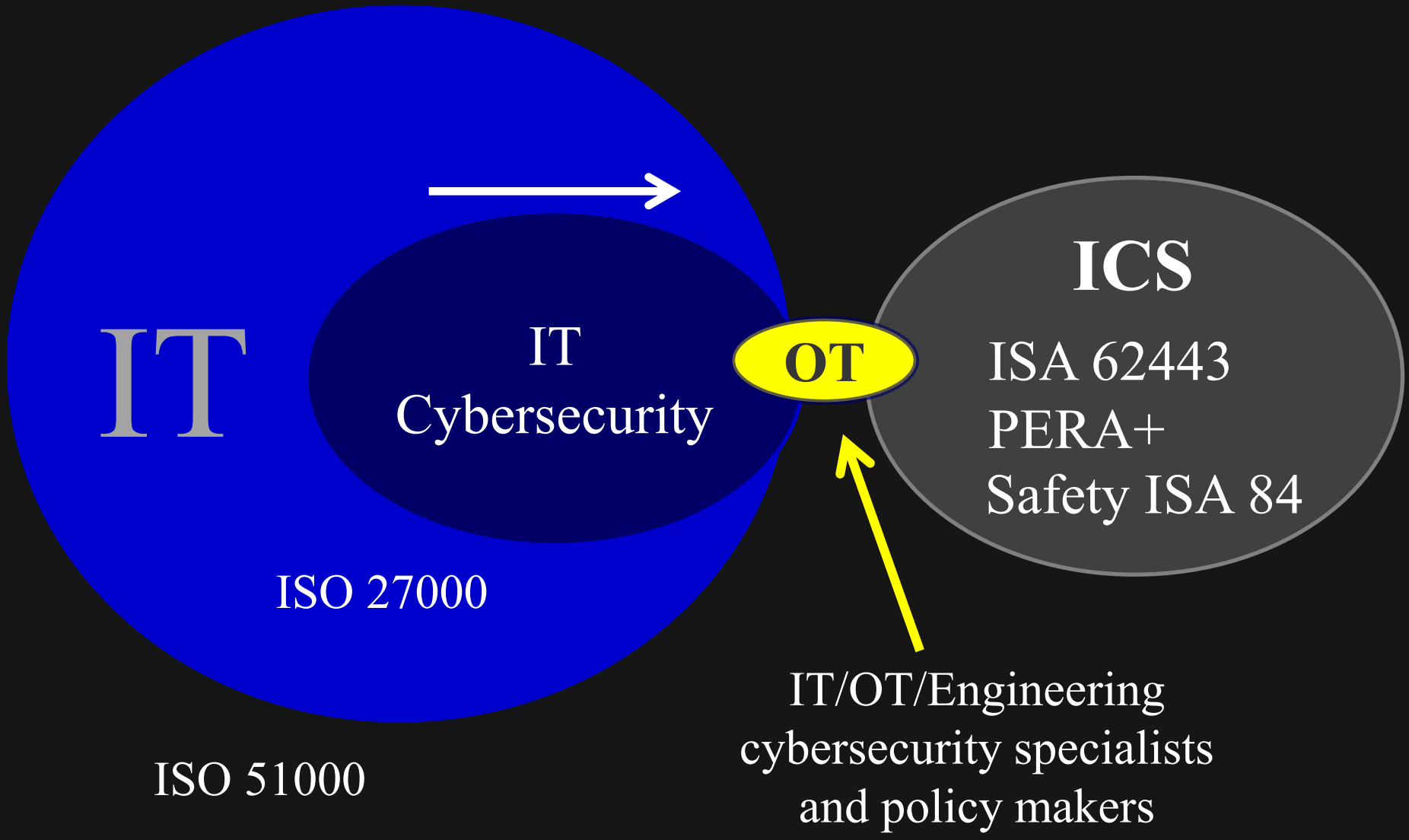
Reflection on 29 December 2025 cyber attack on Polish DER

- Methods and attack vectors known since 2010
- Attacker known since 2015
- Gov/Industry alerts, Reports, Guides (ENISA, OSCE, IEA)
- Best practices available (IEC 61850, ISA/IEC 62443, ISA 84, 95, PERA+)
- Still, victim used (uses) defaults, available security not enabled !

"A cyber-related condition whereby a threat, or warning of a possible threat, results in either the misinterpretation or misunderstanding of a given situation, resulting in a decision in which no corrective action is taken" – V. Butrimas

Author of the word "Cyberg" and site author: Rad Radvanovsky http://cyberg.us/

Need cross-trained engineers to protect CEI



Some content added with the permission of Joe Weiss PE, CISM, CRISC, ISA

Proposal: for enterprise integration look at PERA+

To convey importance of industrial cybersecurity risks to both governments and industrial end users.

Help determine what is critical for risk assessment

To inform Owners, Vendors, and Service Providers on integrating cybersecurity requirements set by governments, regulatory groups, and end user groups.

To inform educators about the necessary skills needed for existing staff and new graduates.

To access Master Planning User Guides, Learning Maps and Micro Learning Modules to chart a practical path forward.

It is available for FREE !

https://pera.net/

Thanks to Gary Rathwell

Invite engineers to help in CIP Policy Making

…”It is worrying when the engineering community that is running the power grid, petrochemical plants, and water systems is not represented.”

https://www.gov.si/en/news/2021-09-06-bled-cybersecurity-conference/

https://scadamag.infracritical.com/index.php/2020/10/16/tale-of-two-conferences-on-protecting-critical-infrastructure-it-was-the-best-of-times-it-was-the-worst-of-times/

The end