Should they (we) have known better?

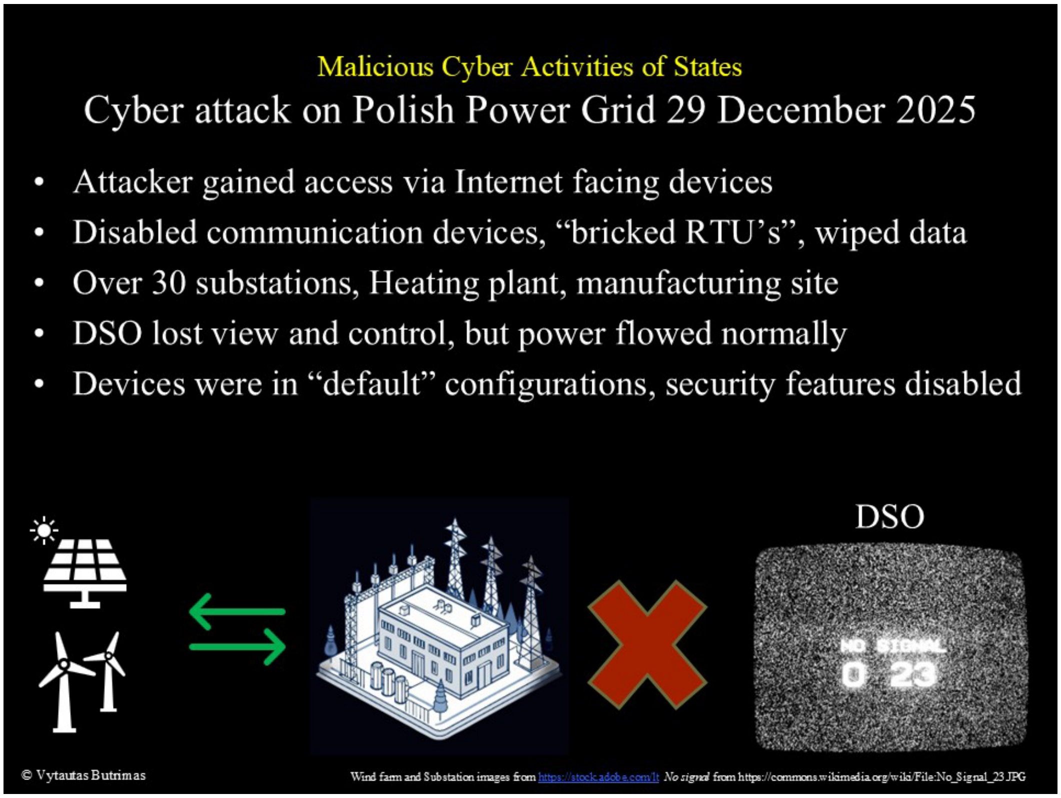
Vytautas Butrimas

NOTE: The views expressed within this blog entry are the author's and do not represent the official view of any institution or organization affiliated thereof.

Article was originally posted on SCADASEC website General Topic 21-February-2026

In thinking about 29 December 2025 cyber-attack on part of the power grid in Poland, one issue at once comes out: THEY SHOULD HAVE KNOWN BETTER!

The methods and attack vectors have been known since 2010 (Stuxnet), the attacker has been known since 2015 (GRU first Ukraine attack December 2015 and again in 2016), Alerts, reports, books have been released about these attacks (CISA, Dragos, Govts, Kim Zetter, Andy Greenberg, etc.) and best practices have been available for decades (PERA, ISA 62443, 95, 88), yet the victim used default configurations with some available security settings not enabled! Not the best security choice to make when it is believed that the responsible suspect nation is engaged in a brutal aggression across the border.



Malicious Cyber Activities of States

Cyber attack on Polish Power Grid 29 December 2025

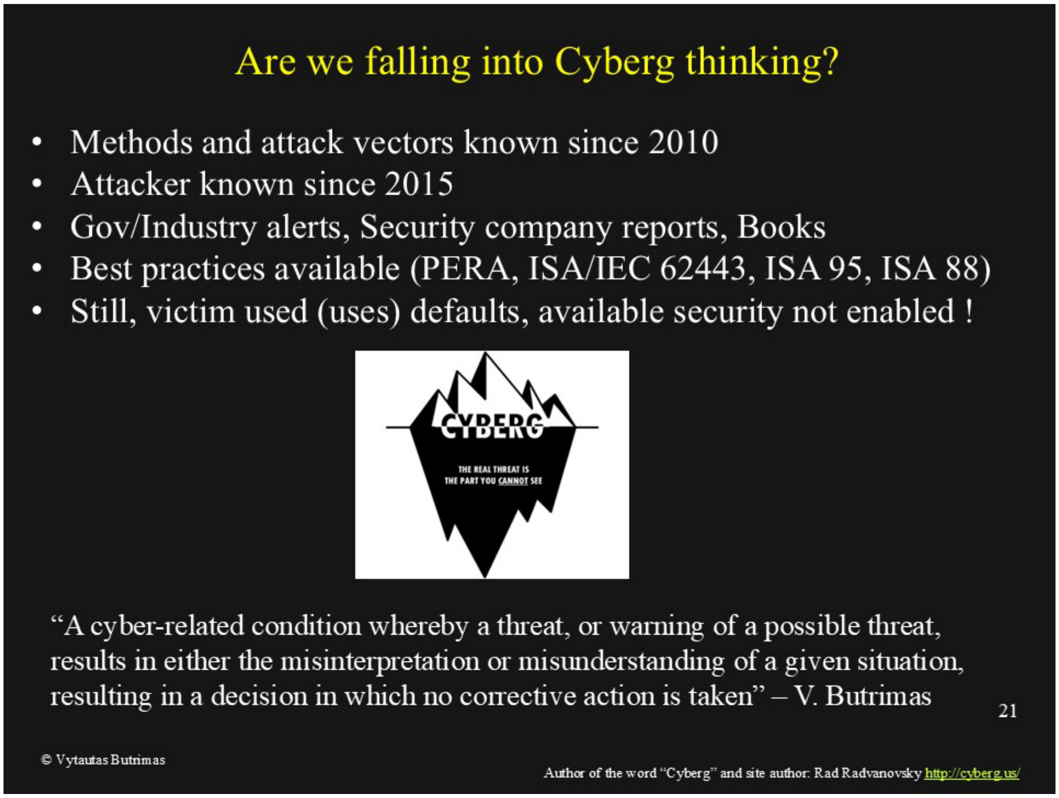
- Attacker gained access via Internet facing devices
- Disabled communication devices, "bricked RTU's", wiped data
- Over 30 substations, Heating plant, manufacturing site
- DSO lost view and control, but power flowed normally
- Devices were in "default" configurations, security features disabled

© Vytautas Butrimas

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

One more question raised is what is wrong with the distribution and acceptance of lessons learned? This incident was, according to the publicly available information[1], made possible by the attacker simply reaching for the "low hanging fruit" on the victim's control infrastructure. Is it because the victim is afraid to change anything (removing defaults, enabling something after production starts (if so, what was the system integrator thinking about)? Is it a sign that the operator lacks sufficient knowledge of their systems and operation? Training is certainly available that can address the low hanging fruit issue. Or is it cybergs again i.e, … "Things are just fine, no need to send anyone to training, and no need to change what we are used to doing"?

I resist saying this incident is another "wake up call". IMO there have been sufficient alarms not just in this recent case but since 2010.



Are we falling into Cyberg thinking?

- Methods and attack vectors known since 2010
- Attacker known since 2015
- Gov/Industry alerts, Security company reports, Books
- Best practices available (PERA, ISA/IEC 62443, ISA 95, ISA 88)
- Still, victim used (uses) defaults, available security not enabled !

CYBERG
THE REAL THREAT IS THE PART YOU CANNOT SEE

"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

21

© Vytautas Butrimas

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

N.B. One of the definitions of "cyberg" is applied in discussing this incident: "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" – quote (attributed to yours truly and other definitions available on the cyberg website //cyberg.us (special thanks to Rad Radvanovsky).

[1] Link to CERT POLSKA report referred to in this article

https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/?mc_cid=ba8c8a4a98&mc_eid=6d66d59513 .

Vytautas Butrimas has been working in cybersecurity and security policy for over 30 years. He has participated in several NATO cybersecurity exercises, contributed to various international reports and trade journals, published numerous articles and has been a speaker at conferences and training sessions on industrial cybersecurity and policy issues, and has also conducted cyber risk studies of the control systems used in industrial operations. He collaborates with the International Society of Automation (ISA) on the ISA 62443 Industrial Automation and Control System Security Standard and is former Co-chair of ISA 99 Workgroup 16 on Incident Management and member of ISA 99 Workgroup 14 on security profiles for substations.