The cybersecurity dimension of critical [energy] infrastructure

"it appears that someone found remote access and started tripping breakers."

- Scadasec commentator 2015-12-26

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

EPP Brussels
June 7, 2017

Vytautas Butrimas
Cybersecurity SME
NATO ENSEC CoE
Member, CRAC (RRT-Council)

Why cybersecurity should be a priority for protecting CEI ?

In 2006 terrorists carrying bombs tried to damage this facility (Abqaiq) but were met with deadly force at the gate

In 2015 the C3 systems of this power grid were remotely compromised from cyberspace putting ¼ mln. in darkness. (hit by cyber again in 2016 !)

What's happening? IT is coming to ICS/OT

- Was analog, manually controlled, now digital & remotely controlled
- Provided wonderful features and efficiencies for the operator
- Supports modern world but introduced complexity & vulnerabilities
- And: Cyber defense was not included as a requirement in ICS design
- Not understanding the differences in IT/OT will lead to bad policy

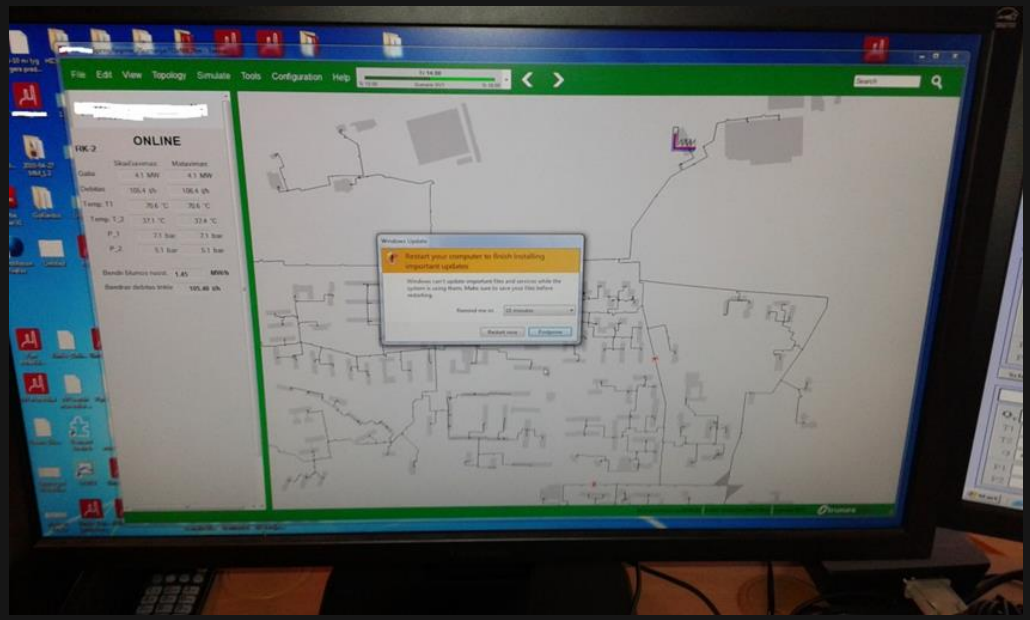
1971

Today

IT introduced new vulnerabilities in ICS / OT world

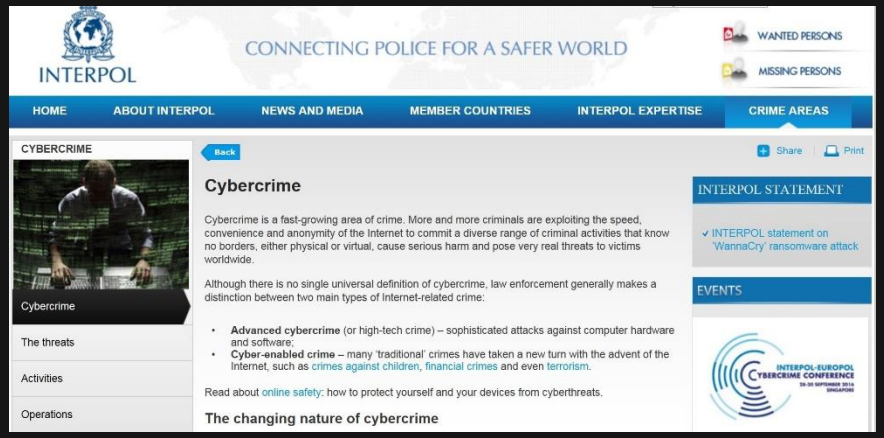
Unintentional / intentional cyber incidents

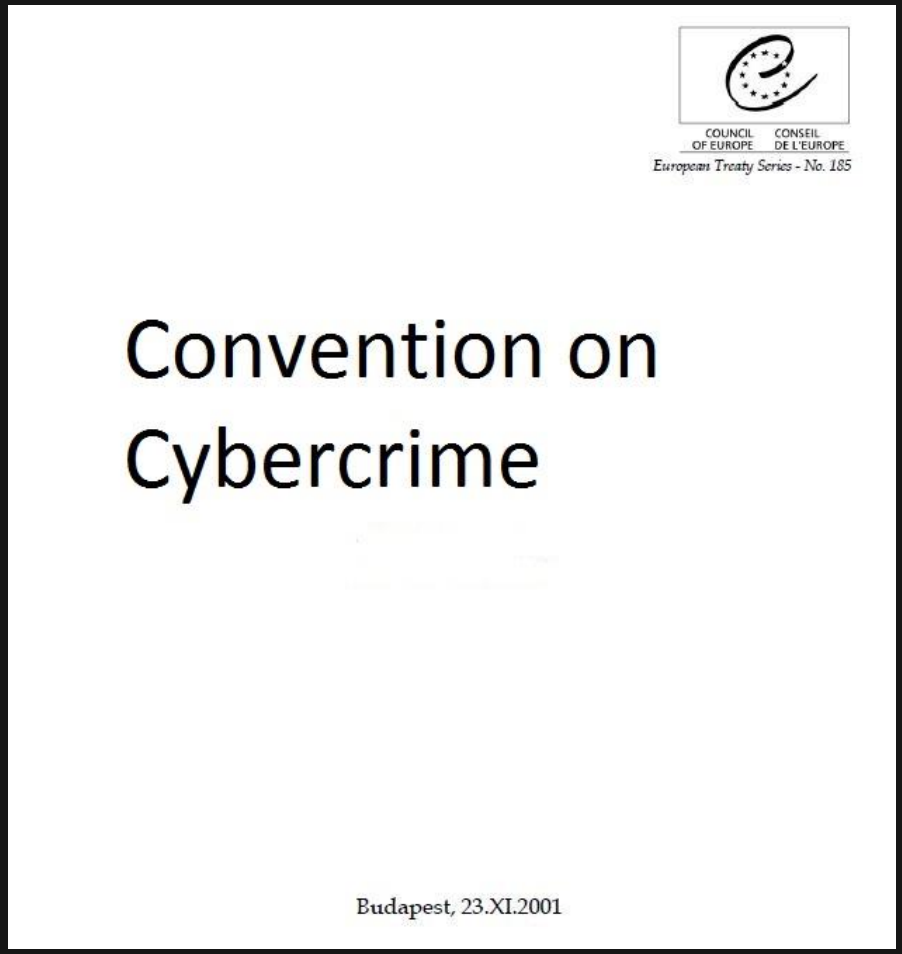
- “A nuclear power plant was recently forced into an emergency shutdown for forty-eight hours after a software update was installed on a single computer”.



How well are we addressing cyber threats?

Great, but is it enough to focus on the cybercrime threat?





Oh, oh a problem:
What to do if it is the work of a STATE?

"But as soon as we find out that it's state-sponsored, or there may be state actors involved, we back away from that."

- Interpol digital crime center director Sanjay Virmani, 2015

Really, are states misbehaving in cyberspace?

- Iranian nuclear and oil facilities (STUXNET 2010)
- Saudi Aramco DOC attack 2012/2013
- Belgacom compromised 2013
- 2013 Sandworm Team / B.E. (ICS Reconnaissance)
- 2014 BSI reports cyber-attack on German steel mill
- 2015 TV5Monde
- 2015/2016 Cyber attack on control systems of Ukraine's pwr grid
- 2017 "WannaCry" as latest "wake-up-call"
- Training is available on how to do this

Implications:

Policy makers have failed to establish cyberspace rules
- “Multi-stakeholder” governance model is obsolete

States, those they sponsor, and less skilled adversaries will continue to see this behavior as

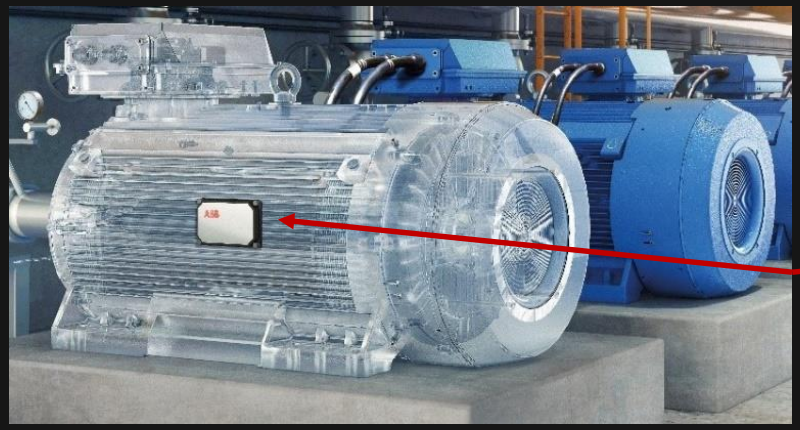
- Effective
- Cheap
- Deniable

Can expect more “wake-up-calls”

The future: More IT/OT convergence, more vulnerabilities

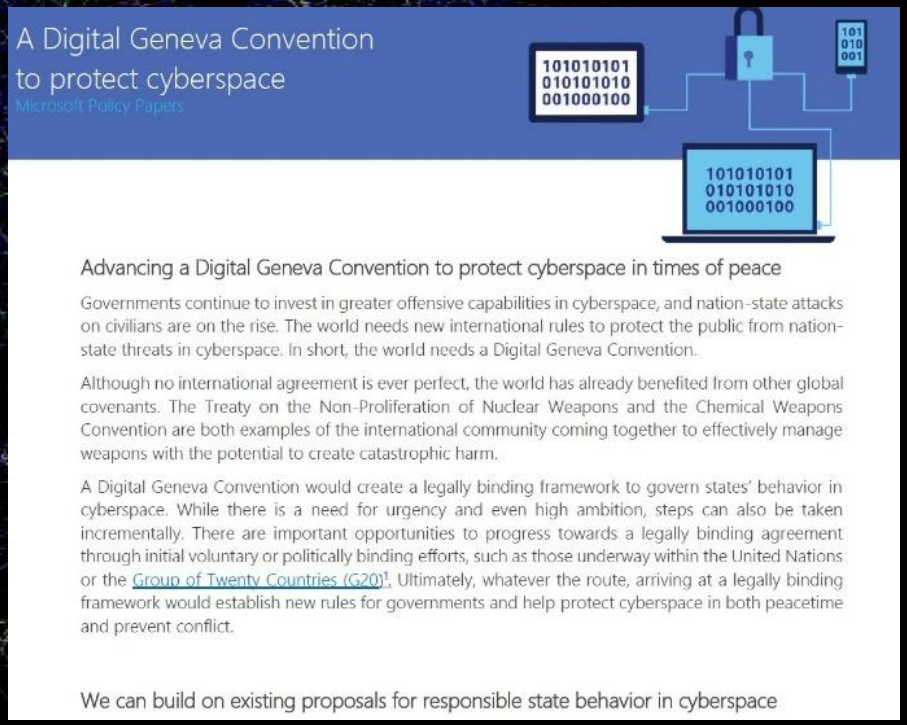
"Caveat emptor"

- "Industry 4.0" integrating manufacturing plant w/ business functions
- IIoT and DA "improve efficiency, reduce downtime and save money"
- Autonomous control and self configuration ?
- Getting a lot of support from Govt. and Industry (€ , $)
- Not much talk about new vulnerabilities and cybersecurity !!!!



Keep in mind, that….

- Protecting IT is not enough, forgetting OT can hurt you
- Fighting cybercrime is not enough, other dangerous actors involved
- Malicious activities of states in cyberspace can affect civilian C.I.
- When developing C.I. policies, don't forget to invite the engineers



Thank you, do you have any questions?

Vytautas Butrimas
NATO ENSEC CoE
Vytautas . Butrimas @ enseccoe . org
Twitter: @ vbutrim
Blog contributor: http://scadamag.infracritical.com/

Thanks to R. Radvanovsky and J. Brodsky for useful suggestions and comments.

Blank slide

Extra slides: if time allows

Questions to consider during presentation

What do you have to protect?

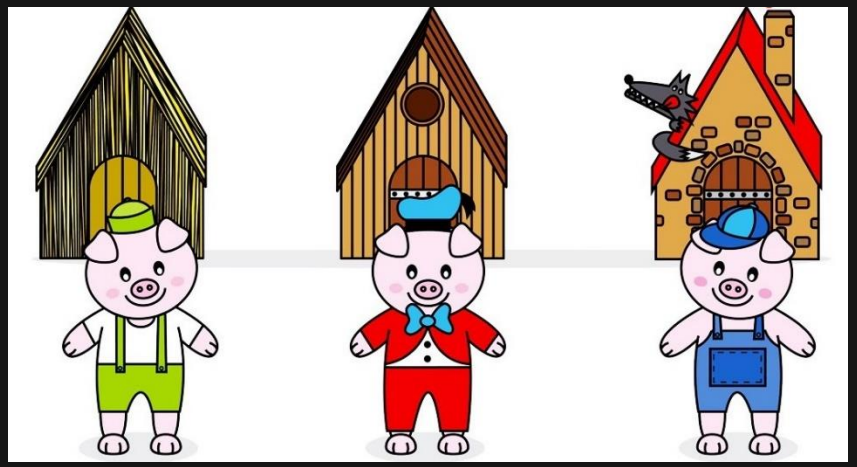
- What is really critical to your operations?

From what threats?

- Can’t protect everything but did you miss something?

How?

- Think lesson of the “3 little pigs”



Energy infrastructure needs protecting because…