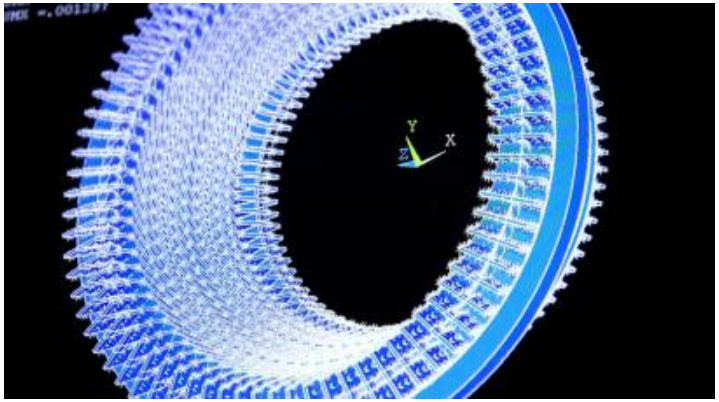
institut français des relations internationales

Cyber attacks: a new threat to the energy industry

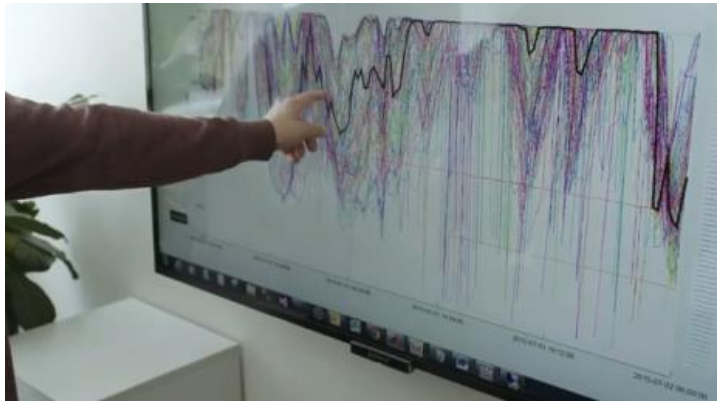
Gabrielle Desarnaud
Research Fellow – Centre for Energy – Ifri

23 February2017

Digitalization and energy



Wind turbine rotor visualization for remote maintenance



Wind turbine data collection and analysis for predictive maintenance

- Digitalization : long term trend in the energy industry accelerating → industrial internet

- Convergence of the global industrial system with the power of advanced computing & analytics

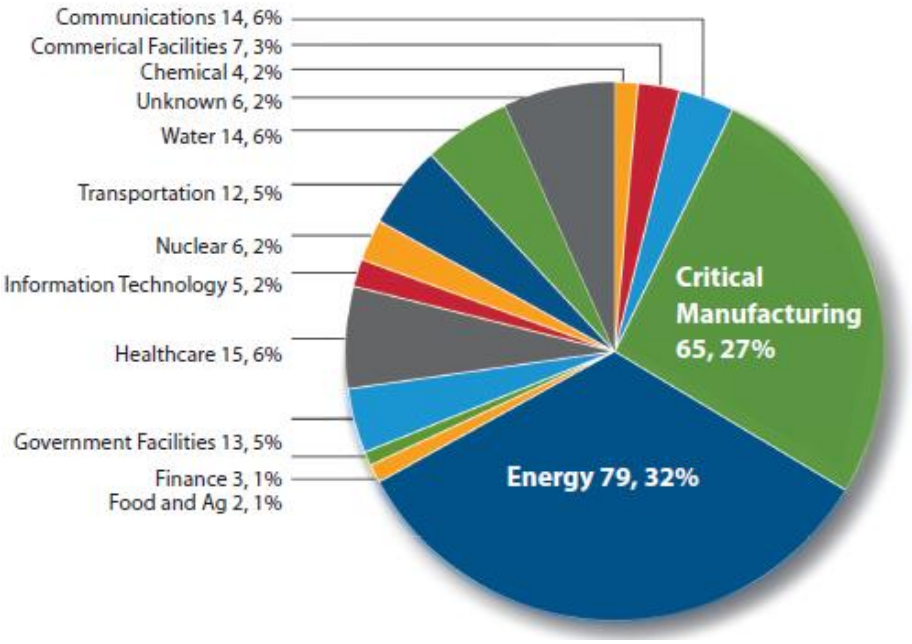
- Allows businesses to leverage big data to optimize processes and asset performance. Apply predictive analytics to minimize unplanned downtime. Increase throughput, improve product quality and drive resource efficiency.

- North America: 1% savings in utility operating costs represents annual savings of $500 million

Cyberattacks in the energy sector

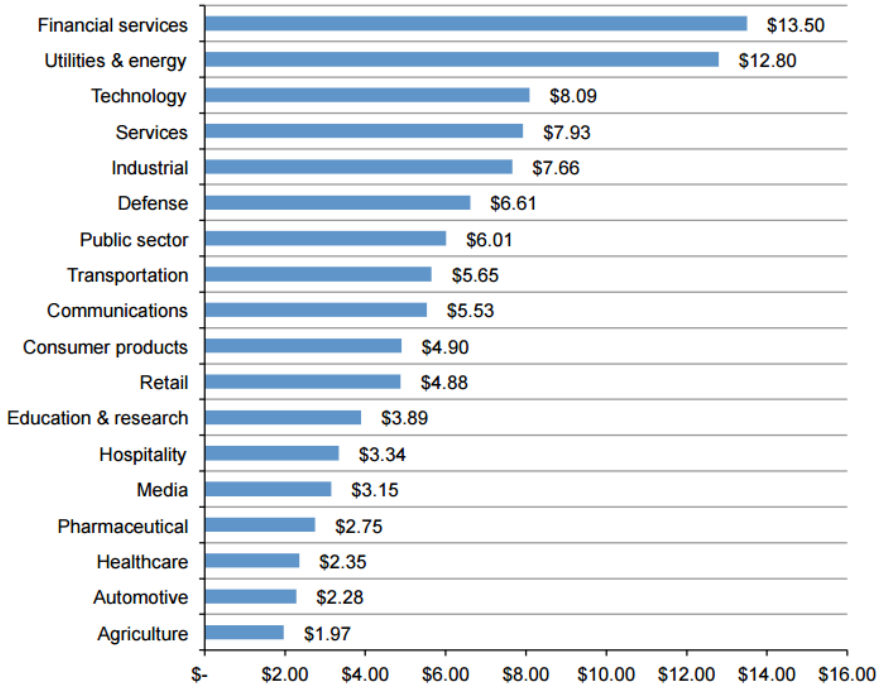
- Attacks against industries since 2010 tend to grow in number and be more sophisticated

Incidents reported to the US Department of Homeland Security in 2014 (Total 245)



Source: US Department of Homeland Security, ICS-CERT Monitor 2014

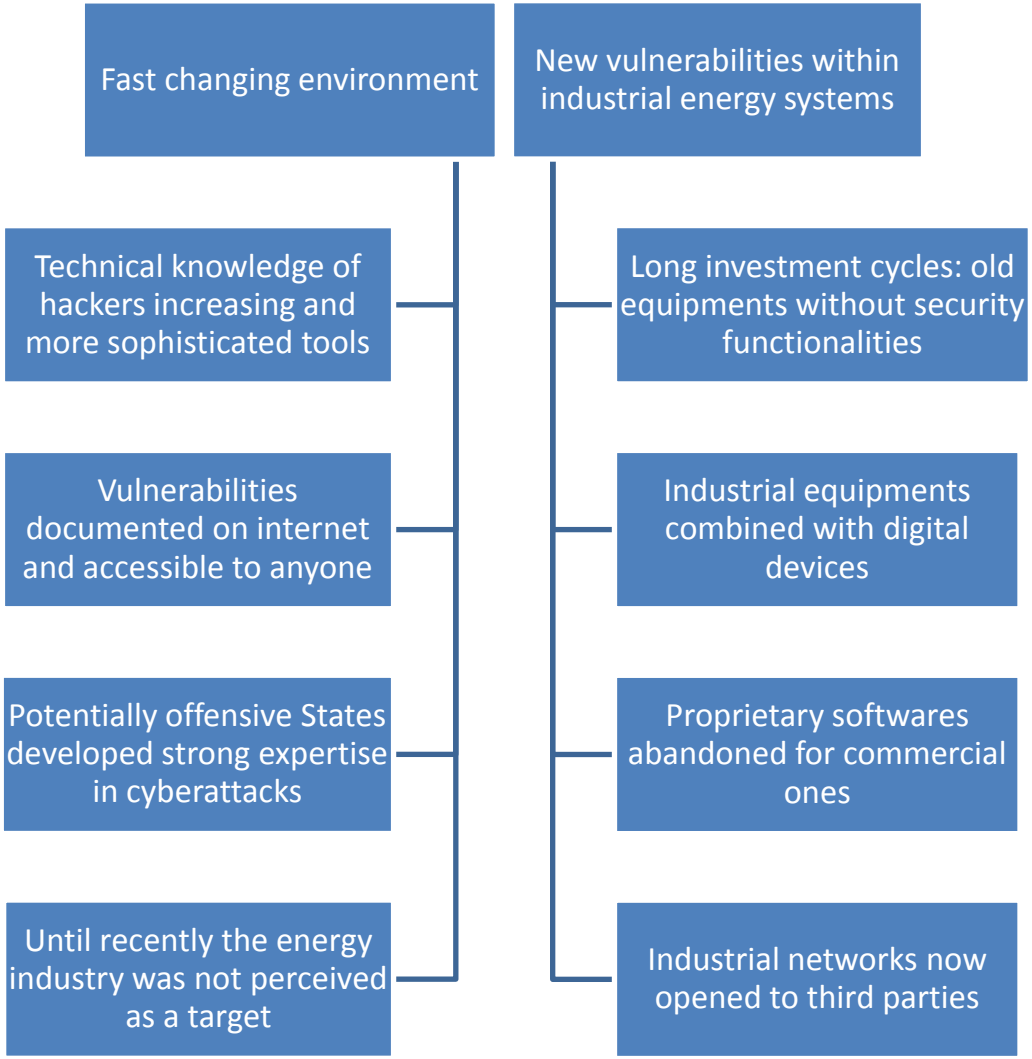
Average annualized cost by industry (2015)



Source: Ponemon Institute 2015

Year	Target	Consequences: cyberattacks against the energy industry
1982	Gas pipeline explosion (Russia)	Malware introduced in the SCADA managing gas flows, explosion equivalent to 3 tons of TNT
1992	Ignalina nuclear plant (Lituania)	A technician of the plant introduced a virus in the ICS of 2 RBMK reactors (Tchernobyl type).
1992	Chevron emergency system (USA)	A dismissed employee of Chevron hacked and deactivated the urgency alert system. Discovered only after an urgency situation appeared in a Chevron refinery in Richmond.
1999	Gas pipeline in Bellingham (USA)	Unvoluntary incident partly linked to the development by Olympic Pipe Line of a database for the SCADA in charge of gas distribution. The subsequent leakage caused 3 death.
2001	California electricity operator (USA)	Attackers accessed the internal network of California Independent System. No injuries.
2003	Davis-Besse nuclear plant (USA)	**Slammer** - The Safety Parameters Display System stopped (no spying of sabotage functionalities)
2008	Hatch nuclear plant (USA)	An update by a consultant rebooted a computer causing an unvolontary shutdown of the reactor for 48 hours.
2010	Natanz (Iran)	**Stuxnet** - Several years of infiltration in Natanz complex of uranium enrichment, more than 900 centrifuges damaged.
2011	Gas and oil industries (Europe-USA)	**Night Dragon** - Gas and oil projects information and contracts stolen
2011	Energy industries	**Duqu** – Parts of the code identical to Stuxnet, made only for industrial espionage.
2011	Areva (France)	Non critical data stolen. Espionage campaign lasted 2years.
2012	Energy companies and institutions (Middle East, North Africa)	**Flame** - Lasted at least 2years. Espionage and data analysis.
2012	Saudi Aramco (Saudi-Arabia)	**Shamoon** - 30 000 hard drives of the compagny destroyed, no damages to industrial networks
2013	Bowman Avenue Dam (USA, NYC)	Attackers took control of the SCI of the small dam, no consequences
2014	250 Energy companies (USA and Western Europe)	**Energetic Bear** - Espionage
2014	Gas stations	**Operation Petrol** - Le groupe d'hacktivistes Anonymous hacktivists group announced they would targe cyberattacks against oil companies and gas stations (DDOS…). No evidence they succeeded
2014	Korea Hydro and Nuclear Power (KHNP) – South Korea	Maps and handbooks of 2 reactors and electrical circuit stolen, as well as data by activists.
2015	Electricity operators - Ukraine	**Black Energy** – About 30 electric substantions shut down, 8 provinces without electricity during several hours, components physically damaged during several weeks

Vulnerabilities in the energy industry

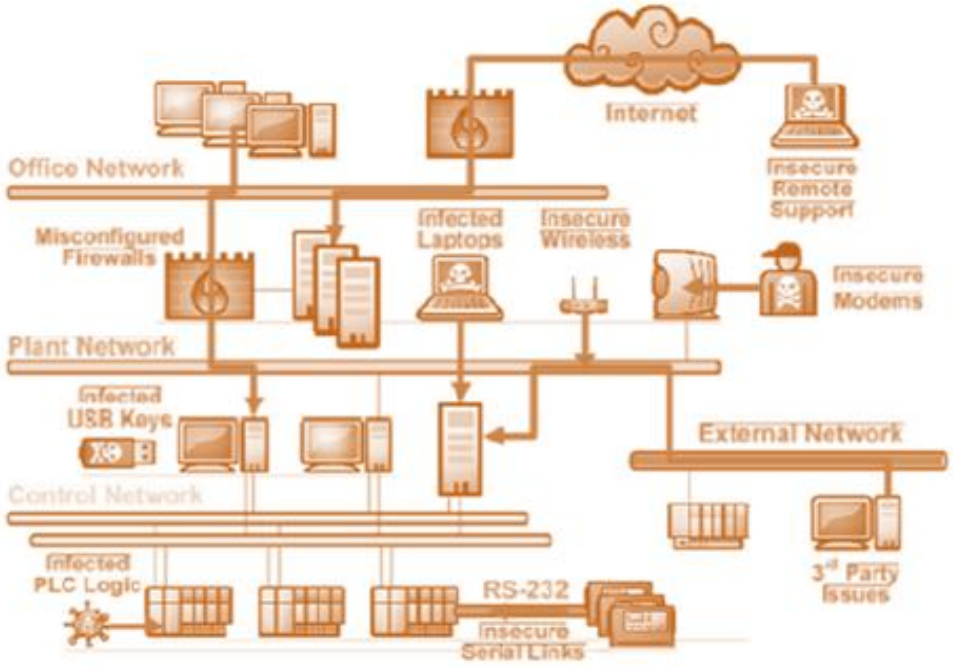


• Improvements to be made in the industry:

- ➢The "air gap"
- ➢Lack of communication/common decisions making between IT and operation branches
- ➢Lack of budget for security
- ➢Internal threat: poor training for employees
- ➢No incidents tracking

- ➢Very few Intrusion Detection Systems and operational Security Operation Center (SOC)

Conclusion: Anticipating the risks



• Some trends are likely to increase the risks in the coming decades :

- Smart meters and smart grids (Spanish smart meters hacked by “white hats”)
- Integration of renewable energy
- Growing grid interconnections
- IoT
- Development of batteries
- Aggregators will grow in number

EU Member States take measures independently, with different approaches:

- France adopted sectorial legislation in cooperation with the industry
- Germany also follows a regulatory approach, although partnerships are better accepted by the industry
- Some States still need to make significant improvements that the NIS directive will foster

institut français
des relations
internationales

THANK YOU FOR YOUR ATTENTION

Gabrielle Desarnaud, desarnaud@ifri.org, @Ifri_Energie

27, rue de la Procession, 75740 PARIS CEDEX 15
Tél. 01 40 61 60 00 • Fax : 01 40 61 60 60