LUT
University

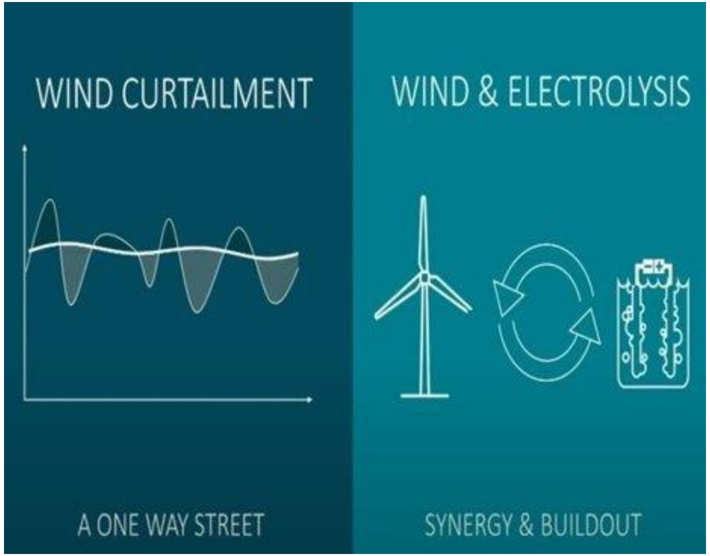
Hygcel 2024

Recommendation on Cybersecurity and Safety in the Hydrogen Economy

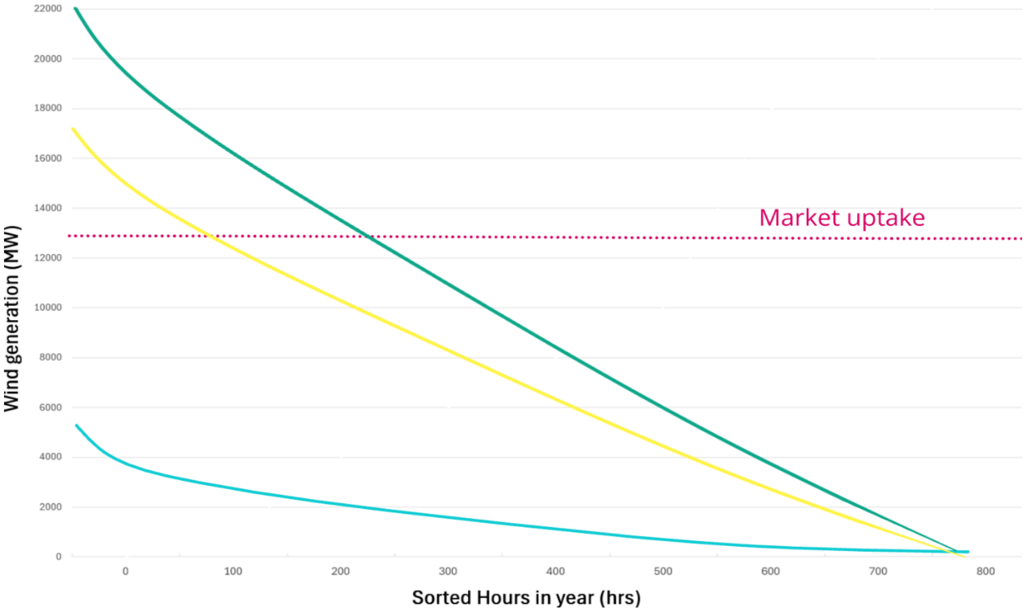
WP 6
Rami Alfasfos
Supervised: Jani Sillman, Risto Soukka

WP 4
Mehar Ullah
Supervised: Pedro Nardelli

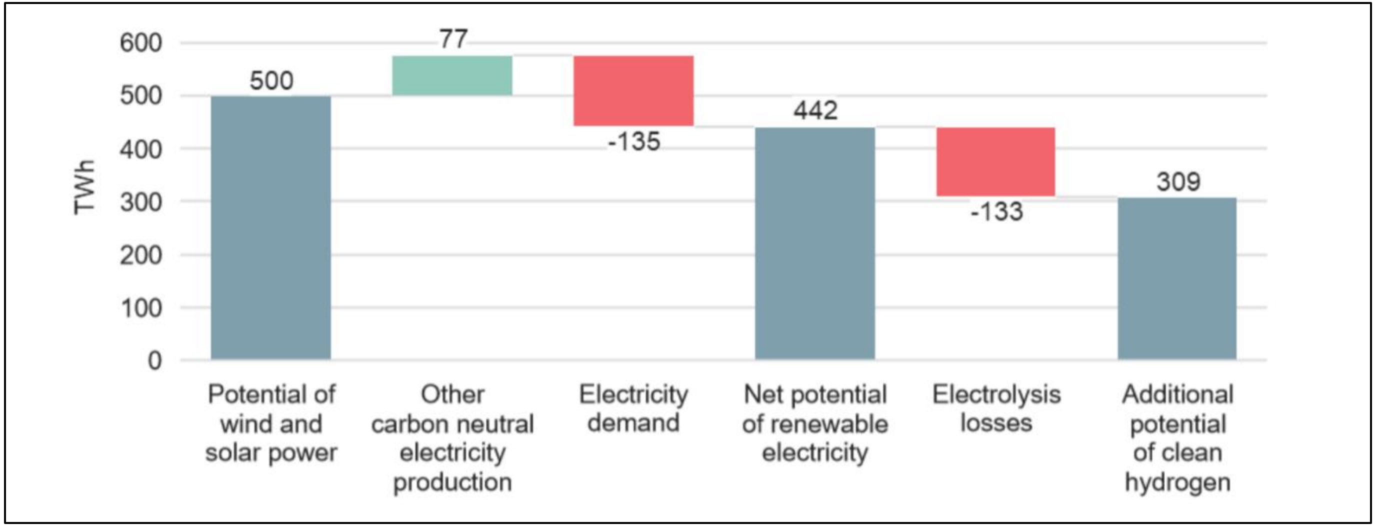
SYNERGY: WIND AND ELECTROLYSIS



This Photo from HHydrogen in pipelines (online workshop)



Clean Hydrogen Production Potential in Finland



This Photo from Fingrid and Gasgrid Finland's joint project

Digitalization of energy systems ”The Digital revaluation”

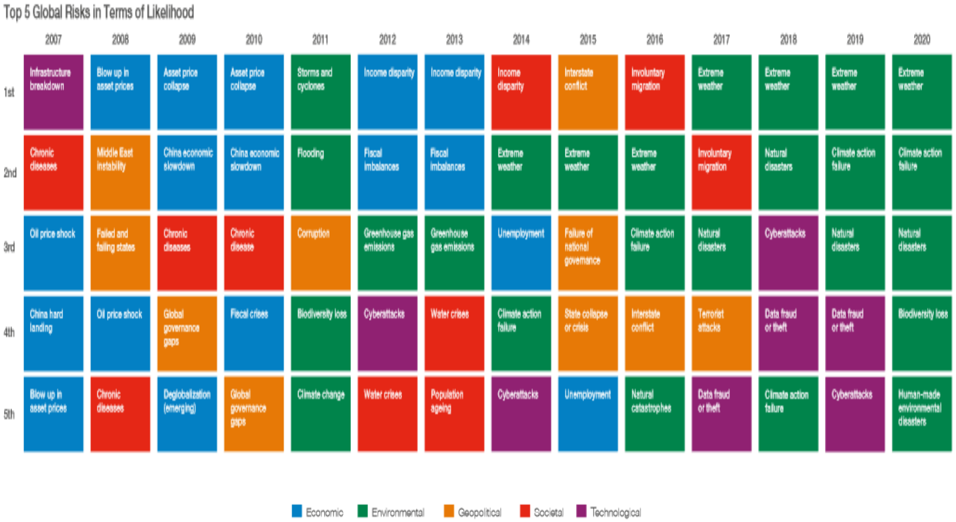
» Digitalization for energy system has added great benefits to the energy system:

+ Ability to connect many devices and energy sources
+ Potentially enhance the efficiency
+ Easier operation and control of an energy systems
+ Cut of cost and accelerate clean energy transition

- **Growing Connectivity:** The rapid increase in connected devices in the energy sector, such as smart appliances, is expanding the potential attack surface for cyberattacks.

- **Cyberattack Vulnerability:** Increased connectivity and automation make electricity systems more vulnerable to cyberattacks, potentially leading to physical damage and service disruptions.

The Evolving Risks Landscape, 2007–2020



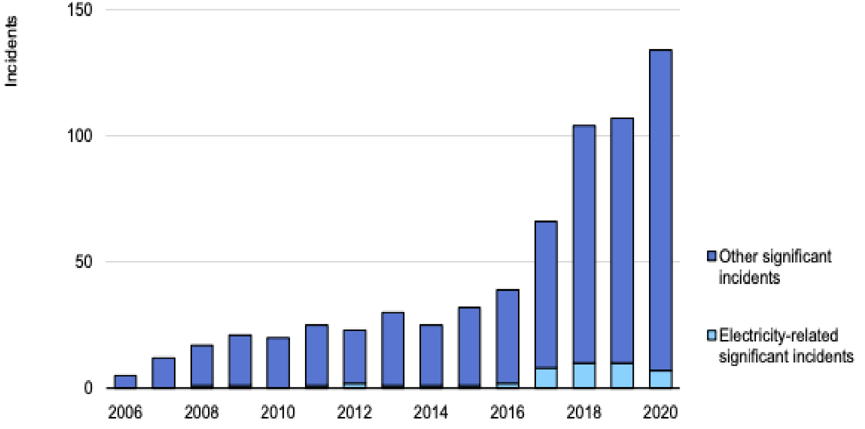
Top 5 Global Risks in Terms of Likelihood

	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
1st	🟪 Infrastructure breakdown	🟦 Blow up in asset prices	🟦 Asset price collapse	🟦 Asset price collapse	🟩 Storms and cyclones	🟦 Income disparity	🟦 Income disparity	🟥 Income disparity	🟧 Interstate conflict	🟥 Involuntary migration	🟩 Extreme weather	🟩 Extreme weather	🟩 Extreme weather	🟩 Extreme weather
2nd	🟥 Chronic diseases	🟧 Middle East instability	🟦 China economic slowdown	🟦 China economic slowdown	🟩 Flooding	🟦 Fiscal imbalances	🟦 Fiscal imbalances	🟩 Extreme weather	🟩 Extreme weather	🟩 Extreme weather	🟥 Involuntary migration	🟩 Natural disasters	🟩 Climate action failure	🟩 Climate action failure
3rd	🟦 Oil price shock	🟧 Failed and failing states	🟥 Chronic diseases	🟥 Chronic disease	🟧 Corruption	🟩 Greenhouse gas emissions	🟩 Greenhouse gas emissions	🟦 Unemployment	🟧 Failure of national governance	🟩 Climate action failure	🟩 Natural disasters	🟪 Cyberattacks	🟩 Natural disasters	🟩 Natural disasters
4th	🟦 China hard landing	🟦 Oil price shock	🟧 Global governance gaps	🟦 Fiscal crises	🟩 Biodiversity loss	🟪 Cyberattacks	🟥 Water crises	🟩 Climate action failure	🟧 State collapse or crisis	🟧 Interstate conflict	🟧 Terrorist attacks	🟪 Data fraud or theft	🟪 Data fraud or theft	🟩 Biodiversity loss
5th	🟦 Blow up in asset prices	🟥 Chronic diseases	🟦 Deglobalization (emerging)	🟧 Global governance gaps	🟩 Climate change	🟥 Water crises	🟥 Population ageing	🟪 Cyberattacks	🟦 Unemployment	🟩 Natural catastrophes	🟪 Data fraud or theft	🟩 Climate action failure	🟪 Cyberattacks	🟩 Human-made environmental disasters

🟦 Economic 🟩 Environmental 🟧 Geopolitical 🟥 Societal 🟪 Technological

Source: World Economic Forum 2007-2020, *Global Risks Reports*.
Note: Global risks may not be strictly comparable across years, as definitions and the set of global risks have evolved with new issues emerging on the 10-year horizon. For example, cyberattacks, income disparity and unemployment entered the set of global risks in 2012. Some global risks have been reclassified: water crises and income disparity were recategorized as societal risks in the 2015 and 2014 *Global Risks Reports*, respectively.

Significant cyber incidents worldwide, 2006-2020



IEA. All rights reserved.

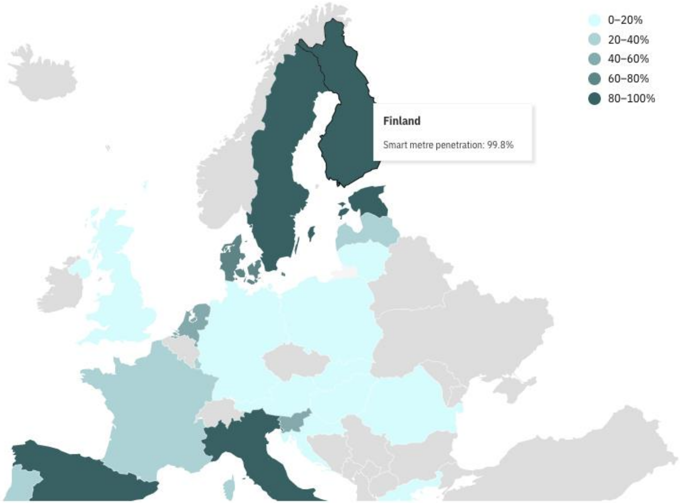
Note: "Significant" cyber incidents are defined as cyberattacks on government agencies, defence and high-tech companies, or economic crimes with losses of more than a USD 1 million.
Source: IEA analysis based on CSIS (2020).

- **Global Cyberattack Threat:** The World Economic Forum's Global Risk Report 2020 lists cyberattacks among the **top ten global risks** in terms of likelihood and impact, signifying their substantial threat to electricity systems.
- **Increased Incidents:** Reports show a dramatic increase in "significant" cyber incidents, with a particular rise in the electricity sector.

Digitalization of Energy Systems

Smart meters make electricity systems more vulnerable to cybersecurity threats

Smart meter penetration by country, 2018 (%)

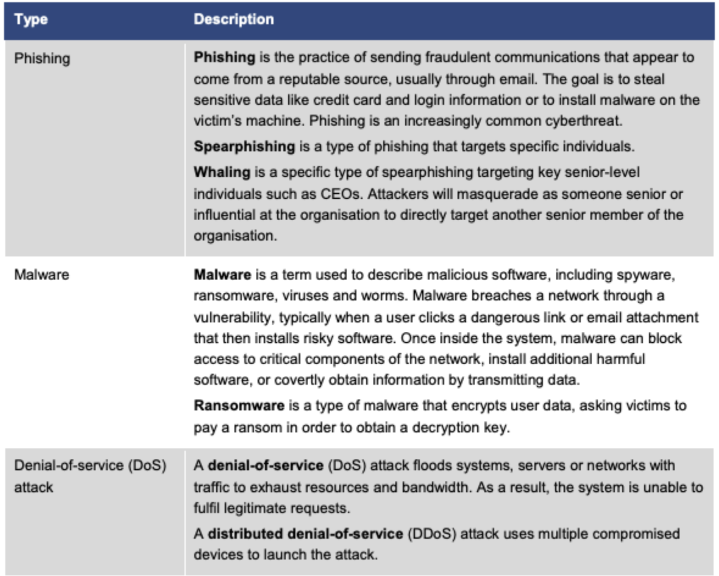


- Smart meters raise questions about the security and data production

- **35 million** Smart meters in France

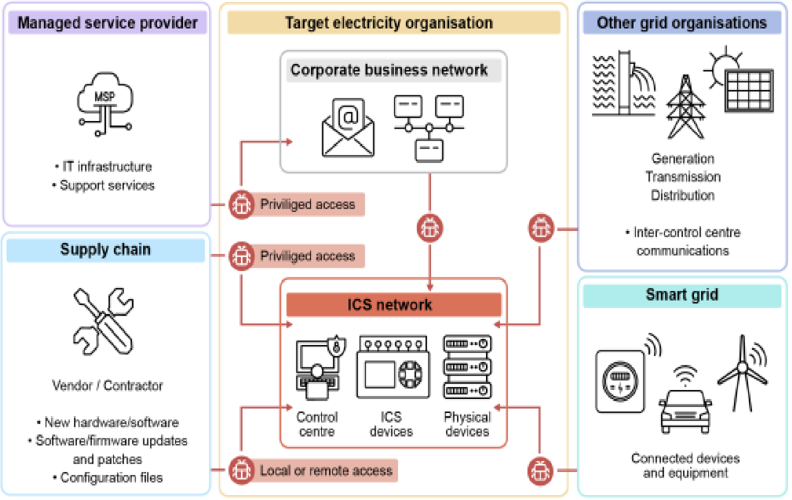
- In Finland approximately **3.7 million** metering point that upgraded with smart technology

Common types of cyberattack on It Systems



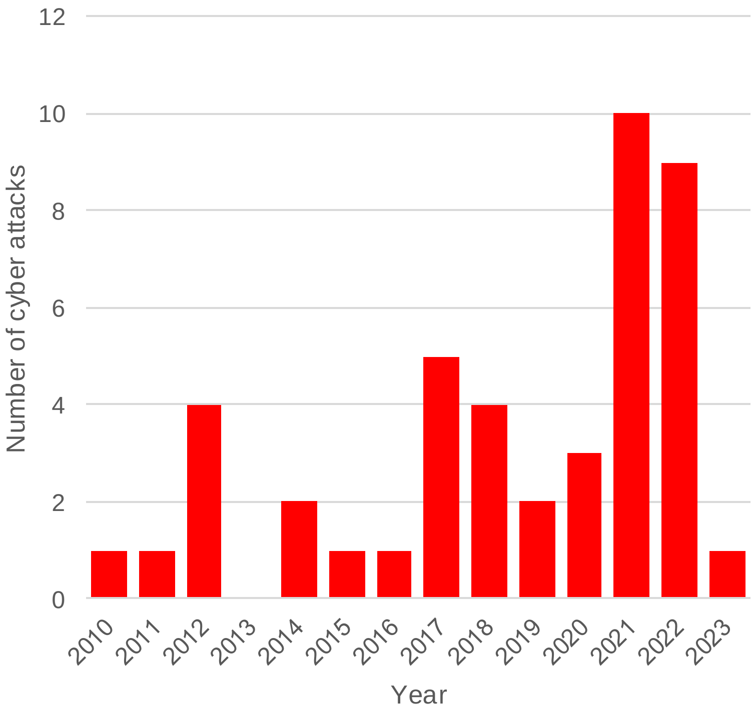
Type	Description
Phishing	**Phishing** is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine. Phishing is an increasingly common cyberthreat. **Spearphishing** is a type of phishing that targets specific individuals. **Whaling** is a specific type of spearphishing targeting key senior-level individuals such as CEOs. Attackers will masquerade as someone senior or influential at the organisation to directly target another senior member of the organisation.
Malware	**Malware** is a term used to describe malicious software, including spyware, ransomware, viruses and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software. Once inside the system, malware can block access to critical components of the network, install additional harmful software, or covertly obtain information by transmitting data. **Ransomware** is a type of malware that encrypts user data, asking victims to pay a ransom in order to obtain a decryption key.
Denial-of-service (DoS) attack	A **denial-of-service** (DoS) attack floods systems, servers or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfil legitimate requests. A **distributed denial-of-service** (DDoS) attack uses multiple compromised devices to launch the attack.

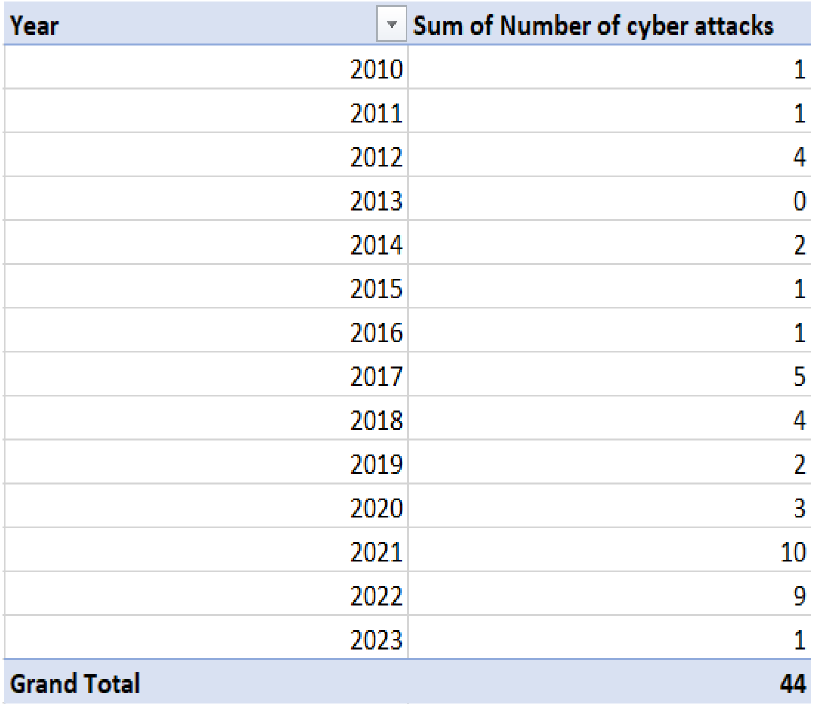
Ways to compromise industrial control systems



Source: Canadian Centre for Cyber Security (2020), Cyber Threat Bulletin: The Cyber Threat to Canada's Electricity Sector – Canadian Centre for Cyber Security.

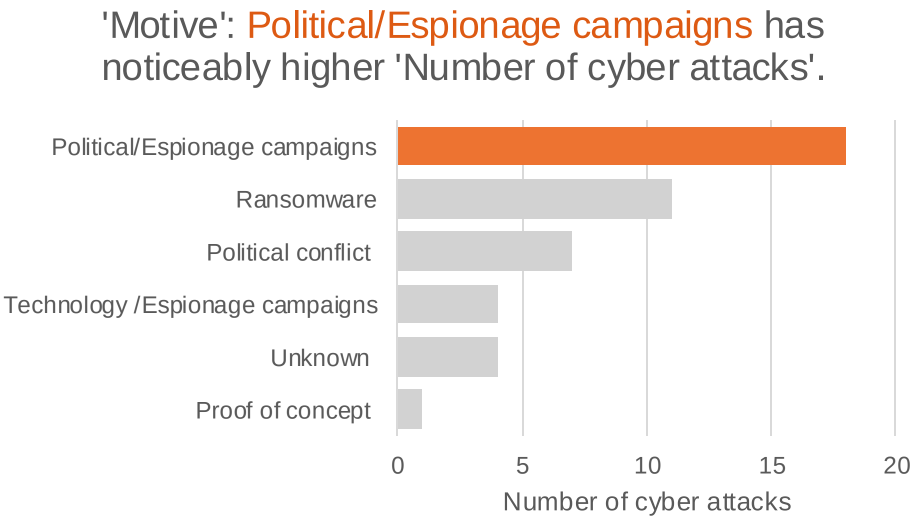
Analysed cyberattacks in the energy systems





Year	Sum of Number of cyber attacks
2010	1
2011	1
2012	4
2013	0
2014	2
2015	1
2016	1
2017	5
2018	4
2019	2
2020	3
2021	10
2022	9
2023	1
Grand Total	**44**

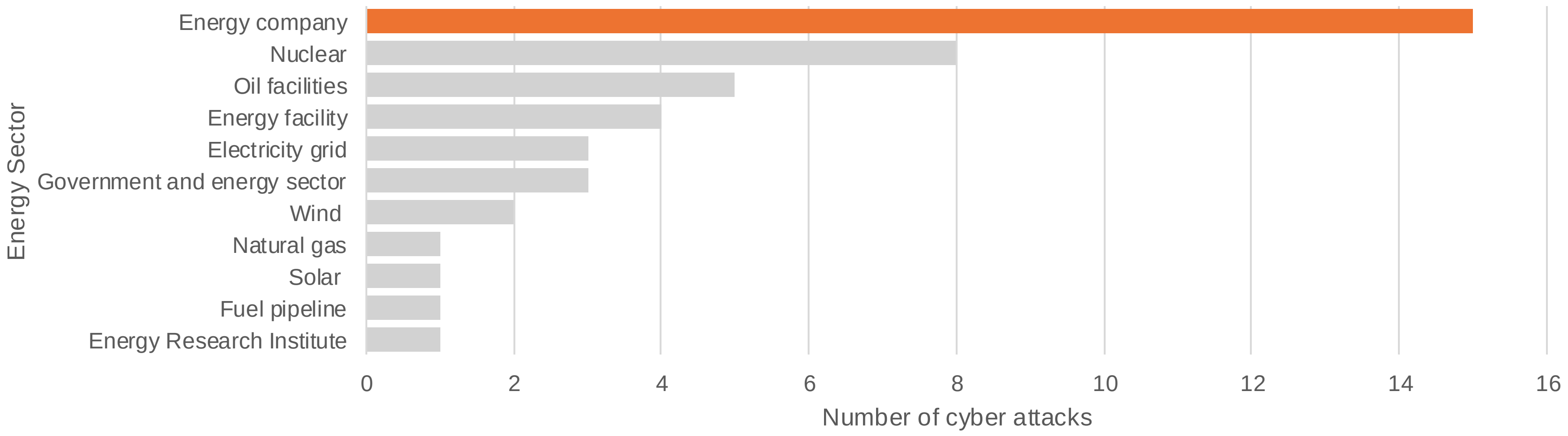
Motive of Cyber-attacks on the energy sector



- **Ransomware and Data Theft:** The energy sector is exposed to common threats like data theft, billing fraud, and ransomware, which can result in significant financial losses.
- **Nation-State Threats:** Nation-state actors are targeting infrastructure providers, posing significant threats to critical infrastructure.
- **Cybercriminal Profit Motive:** Cybercriminals are targeting utilities for profit, often disrupting daily operations and demanding substantial ransoms.

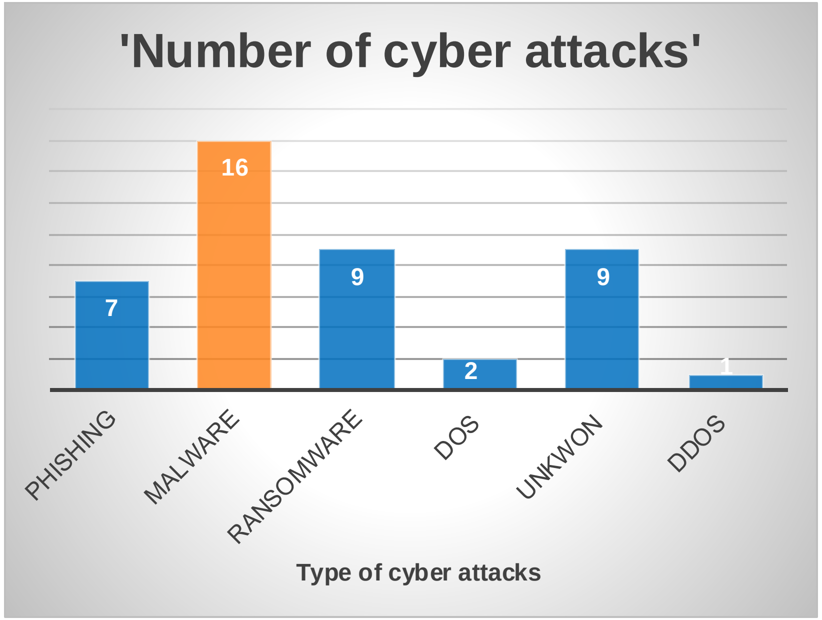
Cyber-attacks on energy sectors

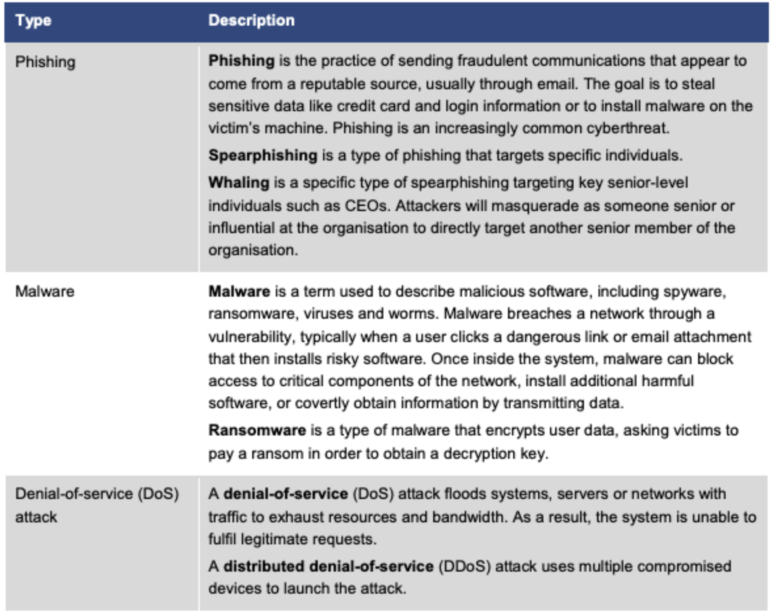
'Energy Sector': Energy company has noticeably higher 'Number of cyber attacks'.



- **Financial Consequences:** Successful cyberattacks can result in significant financial losses for utilities, including costs associated with detection, investigation, containment, recovery, and business disruption.

Sum of Number of cyber-attacks by type





Type	Description
Phishing	**Phishing** is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine. Phishing is an increasingly common cyberthreat. **Spearphishing** is a type of phishing that targets specific individuals. **Whaling** is a specific type of spearphishing targeting key senior-level individuals such as CEOs. Attackers will masquerade as someone senior or influential at the organisation to directly target another senior member of the organisation.
Malware	**Malware** is a term used to describe malicious software, including spyware, ransomware, viruses and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software. Once inside the system, malware can block access to critical components of the network, install additional harmful software, or covertly obtain information by transmitting data. **Ransomware** is a type of malware that encrypts user data, asking victims to pay a ransom in order to obtain a decryption key.
Denial-of-service (DoS) attack	A **denial-of-service** (DoS) attack floods systems, servers or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfil legitimate requests. A **distributed denial-of-service** (DDoS) attack uses multiple compromised devices to launch the attack.

Major Cyber-attacks on energy sectors

Stuxnet worm

Stuxnet is a computer worm reportedly destroyed numerous centrifuges in **Iran's Natanz** uranium enrichment facility by causing them to burn themselves out. Over time, other groups modified the virus to target facilities including water treatment plants, power plants, and gas lines.

It generated a flurry of media attention after it was discovered in 2010 because it was **the first known virus to be capable of crippling hardware**

Source: Satellite images of Natanz show a 10-metre crater © Maxar Technologies/Reuters

Cyber-attacks on energy sectors

BlackEnergy Malware

In December 2015, a first-of-its-kind cyber-attack cut the lights to 225,000 people in western Ukraine, with hackers also sabotaging power distribution equipment, complicating attempts to restore power.

The attacks against Ukraine’s power grid are widely seen by experts as the first examples of hackers shutting off critical energy systems supplying heat and light to millions of homes.

Photo: alexlmx/Adobe Stock

Cyber-attacks on energy sectors

Shamoon wiper worm

The Shamoom Malware story began back in 2012 and 2016 with reports of a data-destroying virus that was completely wiping out the hard drives of tens of thousands of computers at Saudi Aramco.

Shamoon breached computers and destroyed over 30,000 hard drives using a direct drive access driver called RawDisk.

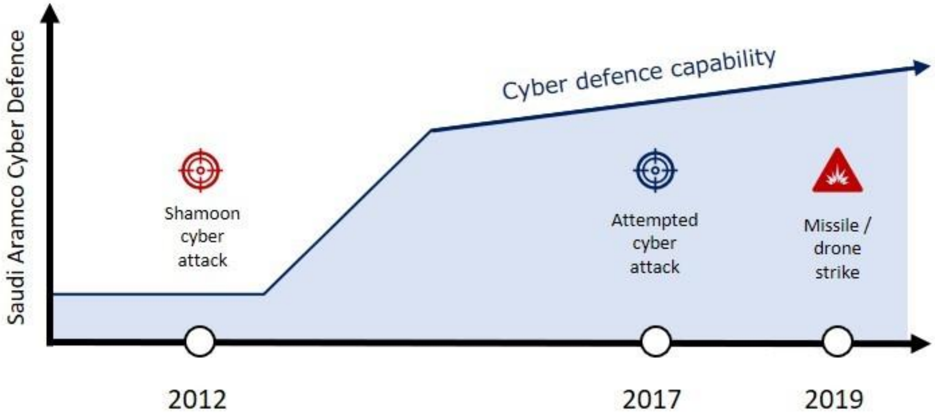
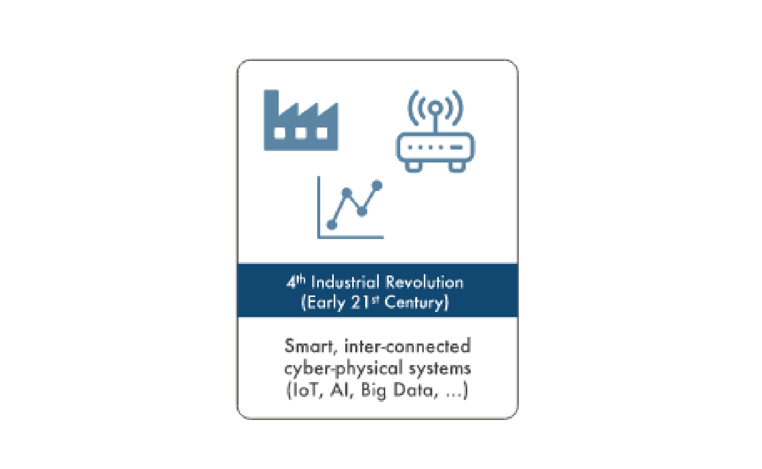


Image source

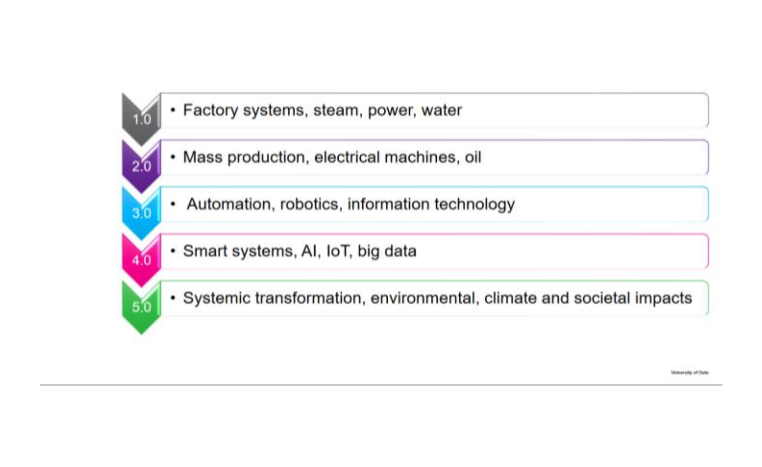
Industrial revolution 4.0

Industrial revolutions



4th Industrial Revolution (Early 21st Century)

Smart, inter-connected cyber-physical systems (IoT, AI, Big Data, ...)



1.0
- Factory systems, steam, power, water

2.0
- Mass production, electrical machines, oil

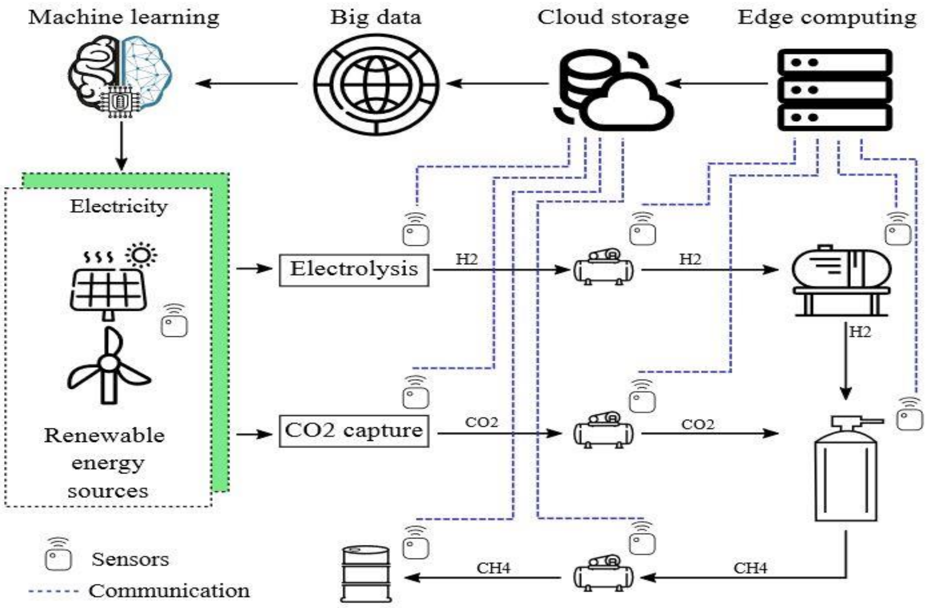
3.0
- Automation, robotics, information technology

4.0
- Smart systems, AI, IoT, big data

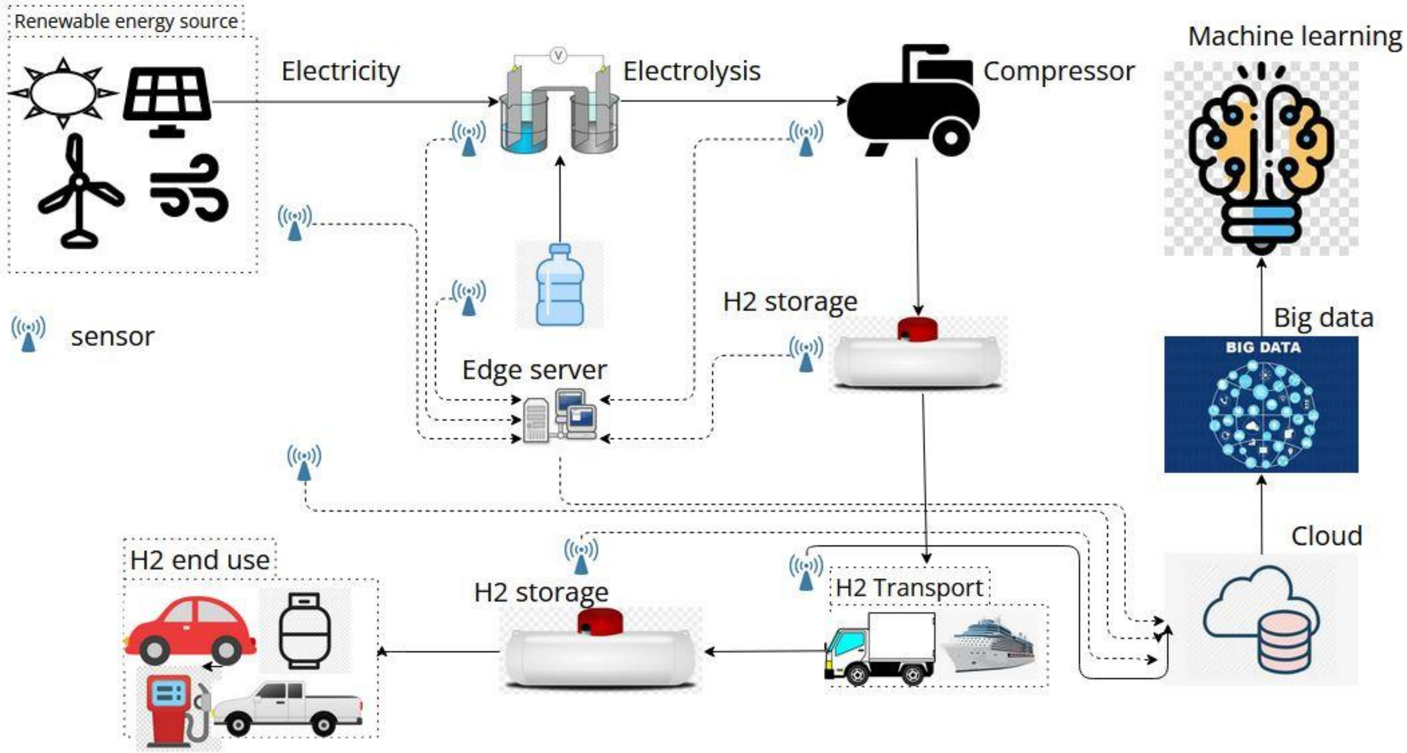
5.0
- Systemic transformation, environmental, climate and societal impacts

University of Oslo

Architecture of Cogeneration plant using latest technologies



Using Edge in Green Hydrogen production



LUT University