No 343 | AUGUST - SEPTEMBER 2021

INSTITUTE OF ENERGY
FOR SOUTH-EAST EUROPE

SEE ENERGY BRIEF:

Monthly Analysis

The Rising Threat of Cyberattacks on the Energy Sector – The Case of SE Europe

Introduction

Electricity is an integral part of all modern economies, supporting a wide range of critical services, including health care, the internet and transportation. The secure of uninterruptible supply of electricity is thus of paramount importance. Digitalisation is rapidly transforming the electricity system, bringing many benefits for businesses and consumers. At the same time, increased connectivity and automation could raise risks to cybersecurity and the threat of cyberattacks. A successful cyberattack could trigger the loss of control over devices and processes in energy systems, in turn causing physical damage and widespread service disruption.

Recent estimates show that overall energy Information Technology (IT) and cybersecurity software and services spending globally is expected to rise from $19 billion in 2020 to $32 billion in 2028 **(1)**. Only about 7% of this is security-related, representing around $1.3 billion in 2020, though this component is proportionally growing faster. **(2)**

The aim of the present "Monthly Analysis" is to highlight a number of past cyberattacks in various energy sectors, including incidents in electricity companies, oil and gas pipelines as well as nuclear power plants on a global and SE European basis and underline the need of taking appropriate precautionary measures in order to strengthen the existing ones and avoid similar situations in the future.

A Global Overview of Cyberattacks in the Energy Sector

Oil and gas pipelines

On May 7, 2021, a cyberattack prompted US Colonial Pipeline, a firm headquartered in Georgia, but operating oil and gas pipelines across USA, to shut down a pipeline stretching from Texas to New Jersey that supplies about 45% of the petrol and diesel used on the east coast. Federal officials confirmed that DarkSide, a ransomware gang believed to be based in the former Soviet Union, was responsible. On May 12, Colonial Pipeline said it had "initiated the restart of pipeline operations", a carefully worded statement that conveys both the difficulty of returning to normal and a desire to contain panic. That day average petrol prices topped $3 a gallon for the first time since 2014. **(3)**

The ransomware attack striking Colonial Pipeline should be a startling lesson in the vulnerability of critical infrastructure to cyber-risks. Like it or not, governments and businesses must adjust to a continually escalating threat environment. As governments contend with the geopolitics of cyberattacks, we can expect many will explore new regulations, expanded cooperation between governments and the private sector, and enhanced technological protections for critical infrastructure. Yet oil and gas executives cannot wait on

government to forge ahead with the daunting task of reducing cyber-risk across their expansive and complex organizations, the World Economic Forum supports. **(4)**

Earlier, in February 2020, the US Department of Homeland Security issued an alert about a ransomware attack that brought down a US gas compressor facility for two days. The agency did not say which facility was targeted, when the attack occurred or who was behind it. But it did offer some details: hackers sent emails with a malicious link, known as a phishing attack, to gain control of the facility's information technology system. **(5)**

In November 2019, Mexico's oil giant Petroleos Mexicanos (Pemex) reported a cyberattack that crippled its computer systems. The company's communication systems were affected for weeks afterwards. For some employees, internet access was limited, some computer files were not accessible and they had difficulty receiving external emails, people in Pemex's finance, legal and refining departments said at the time. The hacker behind the attack tried to squeeze almost $5 million out of the company. Pemex at the time refused to pay the ransom. **(6)**

In April 2018, several US gas pipeline operators, including Energy Transfer Partners LP and TransCanada Corp., reported that a third-party electronic communications system had been hit with a cyberattack. Five of the companies confirmed service disruptions from the hacking. Though the cyberattack did not disrupt the supply of gas to US homes and businesses, it showed how even a minor attack can have ripple effects. The attack forced utilities to warn of widespread billing delays and made it difficult for analysts and traders to predict a key government report on gas stockpiles. **(7)**

In 2012, Saudi Arabia blamed unidentified people based outside the kingdom for a cyberattack against state-owned Saudi Arabian Oil Co. that aimed to disrupt production from the world's largest exporter of crude. More than 30,000 computers were compromised or affected by a so-called "spear-phishing" attack, raising concerns about the threat hackers may pose to output at the company also known as Saudi Aramco. A spokesman for the Interior Ministry declined at the time to identify any of the "several foreign countries" from which the attack originated. **(8)**

Intense market pressure continues to drive a digital revolution in the oil and gas sector. The COVID-19 pandemic added a surge of remote work arrangements to the growing wave of digitized, networked systems that maximize efficiencies and minimize emissions. The clear competitive advantages of digital assets means the digital revolution will continue. More and more of the industrial processes crucial to the oil and gas sector will rely on networked, digitally controlled equipment. Yet the very nature of digitized equipment brings increased cyber-risk. The same tools, which help oil and gas infrastructure run efficiently and support remote operation, are potential points of exposure for cyberattacks.

In part because of the expanded and altered attack surface offered by digitized equipment, the frequency and sophistication of attacks continues to rise, and has shifted focus. Where past attacks focused on IT, attacks focusing on operating technologies are now common. This threat environment is the new normal for oil and gas infrastructure. Whether attackers are criminals motivated by financial gain or nation-state actors playing geopolitics, digitized oil and gas infrastructure makes a tempting target. Board members – and the information security officers they hold accountable – should be preparing for frequent, sophisticated attacks to be an ongoing operational risk. Even for industry leaders keenly aware of the risks and trends facing the oil and gas industry, building robust cybersecurity can be a daunting challenge.

Electricity grids

The European Network of Transmission System Operators for Electricity (ENTSO-E) became one of the latest power sector organisations to have fallen victim of a cyberattack. ENTSO-E, which represents 42 European transmission system operators in 35 countries, announced on March 9, 2020 that it had recently "found evidence of a successful cyber intrusion into its office network" and was introducing contingency plans to avoid further attacks. According to French think-tank IFRI, the power sector has become a prime target for cyber-criminals in the last decade, with cyberattacks surging by 380% between 2014 and 2015. Motives include geopolitics, sabotage and financial reasons. **(9)**

In June 2019, the New York Times reported that the US launched cyberattacks into the Russian power grid. According to the newspaper, US military hackers used American computer code to target the grid as a response to the Kremlin's disinformation campaign, hacking attempts during the 2018 mid-term elections and suspicions of Russia hacking the energy sector. The story was condemned by President Trump, who said it was fake news, while the Kremlin said that it was a possibility. According to the 2018 National Defence Authorisation Act, government hackers are permitted to carry out "clandestine military activities" to protect the country and its interests. **(10)**

In December 2016, hackers took down almost a quarter of Ukraine's power grid. Officials blamed Russians at the time for tampering with the utilities' software and then jamming the power companies' phone lines to prevent customers from calling the alarm. The hack knocked out at least 30 of the country's 135 power substations for about six hours. Cybersecurity firms working to trace its origins say the attack occurred in two stages. First, hackers used malware to direct utilities' industrial control computers to disconnect the substations. Then, they inserted a wiper virus that made the computers inoperable. **(11)**

In a separate incident, in December 2015, hackers got into the system of a western Ukrainian power company, cutting power to 225,000 households. A US report into the blackout concluded that a virus was delivered via email through spear-phishing – a technique that sends key employees detailed messages, using

information gathered from social media. The report did not name any perpetrators but experts suggested it was linked to a group of Russian hackers. **(12)**

Nuclear power plants

In April 2021, Iran announced its largest uranium enrichment facility was a target of "nuclear terrorism". A senior official said a blackout at the Natanz plant, home to thousands of gas centrifuges, was an attempt to thwart both Iran's atomic progress and ongoing nuclear talks in Vienna. In the past, Iran has largely blamed Israel for attacks on its nuclear infrastructure. It is worth noting that the United States and Israel have a history of covert collaboration, dating to the administration of President George W. Bush, to disrupt Iran's nuclear programme. The best-known operation under this collaboration, which was code-named "Olympic Games", was a cyberattack disclosed during the Obama administration in 2010 that disabled nearly 1,000 of the 5,000 centrifuges at Natanz. That attack was believed to have set back Iran's enrichment activities by many months. **(13)**

In October 2019, India confirmed that its newest nuclear power plant was the victim of a cyberattack, exposing the vulnerability of one of the country's most critical sectors to cyber espionage. The Kudankulam nuclear power plant was hacked using malware designed for data extraction linked to the Lazarus Group, cyber experts said. The group is known to have ties to two North Korean backed groups. The Nuclear Power Corporation of India Limited confirmed on October 30, 2019 that malware had been identified in the system but said that it was "isolated from the critical internal network". Its assessment is disputed by cyber security experts who say critical information was compromised. **(14)**

In December 2014, South Korean nuclear and hydroelectric company Korea Hydro and Nuclear Power (KHNP) was hacked. Hackers stole and posted online the plans and manuals for two nuclear reactors, as well as the data on 10,000 employees. The US pinned the attack on North Korea but South Korean authorities traced the IP addresses to Shenyang, a city in north-east China. **(15)**

The Case of SE Europe

A 2019 Energy Community study **(16)** concluded that its Contracting Parties have different levels of risks, which are mostly induced by geopolitical situation. In the first group of countries, there are the **Western Balkans' Energy Community Contracting Parties** (i.e. Albania, Bosnia and Herzegovina, Kosovo, Serbia, Montenegro and North Macedonia) that all have by EU standards smaller sized energy markets and are coping with similar, if not the same, cybersecurity issues (risks, incidents). In this group by cybersecurity maturity level the two most advanced countries (i.e. Serbia and Montenegro) may contribute considerably to the regional overall cybersecurity level by cooperating actively with their neighbours. That would lower

the risk of the whole group. If regional cooperation is somehow more deepened with cooperating energy computer security incident response teams (CSIRTs) and joint exercises and early warning system, Energy Community believes that this will put risks at more acceptable levels.

The second group with higher risk levels members are **Georgia** and **Moldova**, which are practically under constant risk of cyber-war type of incidents. Those two countries need more investment in high tech cyberdefence and must engage very skilled professionals to accomplish some kind of progress in managing cyber risks, not to forget active cooperation on cyber issues with friendly neighbours and NATO's cyber capability defence facilities.

In the third group is **Ukraine**, which is a risk assessment story for itself as being in state of hybrid war not only in cyberspace but also for real. The Ukrainian energy market is huge amongst other Energy Community Contracting Parties and of large strategic interest not only for EU but for USA and Russia as well. As Ukraine's cyber risks are of critical levels, the country is managing them fast and in their best knowledge. Nevertheless, all neighbouring countries must be aware of those risks during any kind of cooperation in the energy sector and must adjust their respective systems/processes to be able to handle the same level of risks (this includes Energy Community also).

Apart from the aforementioned SE European countries, there are also Greece and Turkey. More specifically, Greece's Energy Ministry was hit by a cyberattack in early July 2021 and as a result numerous files were "locked", while at the same time "sensitive" documents and data were retrieved **(17)**. Several energy companies, such as PPC, and public institutions in Greece have already taken necessary precautionary measures in order to mitigate, if not eradicate, any attempt of cyberattack. For instance, Greece's IPTO announced on August 27, 2021 an electronic tender for the nomination of a contractor for the provision of services in order to enhance Cybersecurity Resilience of its infrastructure. The total budget amounts to €10.5 million, while the duration of the contract, including warranty and maintenance services, is 5.5 years **(18)**.

Similarly, Turkey seems to be one of the first countries in SE Europe that have already experienced a cyberattack in their electricity grid. More specifically, sources from the country's Energy Ministry claimed in December 2016 that a major cyberattack was the source of the widespread electricity cuts across Istanbul, according to reports in Turkish media. "The attacks were generally aiming to seize Internet sites and secure infiltration," a senior anonymous source said on December 31, as quoted by state-run Anadolu Agency. "Many infiltration attempts to the systems controlling our transmission and electricity producing lines were determined and prevented. The infiltration attempts are indicators of a major sabotage preparation against Turkey's national electricity network," he added. **(19)**

Discussion

Digitalisation offers many benefits both for energy systems and clean energy transition. At the same time, the rapid growth of connected energy resources and devices is expanding the potential cyberattack surface, while increased connectivity and automation throughout the system are raising cybersecurity risks. The threat of cyberattacks on energy systems is substantial and growing. Threat actors are becoming increasingly sophisticated at carrying out attacks. A successful cyberattack could trigger the loss of control over devices and processes, in turn causing physical damage and widespread service disruption.

While the full prevention of cyberattacks is not possible, energy systems can become more cyber resilient – to withstand, adapt to and rapidly recover from incidents and attacks, while preserving the continuity of critical infrastructure operations. Policy makers, regulators, utilities and equipment providers have key roles to play in ensuring the cyber resilience of the entire energy value chain. Policy makers are central to enhancing the cyber resilience of energy systems, beginning with raising awareness and working with stakeholders to continuously identify, manage and communicate emerging vulnerabilities and risks. Policy makers are also ideally placed to facilitate partnerships and sector-wide collaboration, develop information exchange programmes and support research initiatives across the energy sector and beyond. Ecosystem-wide collaboration can help to improve understanding of the risks that each stakeholder poses to the ecosystem and vice-versa.

As more and more cyberattacks are expected to take place in the energy sector in SE Europe, it is high time to set up an effective regional Energy Cyber Security Advisory Committee in order to assess and prevent them. This Committee could work closely with the Energy Community Secretariat, the International Energy Agency (IEA), ENTSOe, ENTSOg and the recently launched SELeNe CC in Thessaloniki. This will be an ad hoc group composed of specialists in different sectors e.g. electricity, energy efficiency and cogeneration, renewables, oil and gas, coal, nuclear and Information Technology. The group will first of all undertake to ascertain cyberattacks in the regional energy sector and then proceed in cataloguing in detail the energy infrastructure involved and also assess the degree of its exposure. Then, the Committee will proceed to chart a strategy for the strengthening and upgrading of energy infrastructure in relation to the broader steps that need to be taken, such as precautionary safety measures.

The overall aim of this initiative will be to prepare a comprehensive report with detailed recommendations, including a roadmap and fully costed proposals for the work that is required in order to ring fence SE Europe’s energy systems and protect them from extreme phenomena of cyberattacks.

References

1. Business Wire (2020), "Navigant Research Report Finds Global Annual Market for Energy IT and Cybersecurity for Software and Services Is Expected to Reach $32 Billion by 2028", https://www.businesswire.com/news/home/20200211005108/en/Navigant-Research-Report-Finds-Global-Annual-Market
2. Walton, R. (2020), "Utilities say they are prepared to meet cyber threats. Are they?", https://www.utilitydive.com/news/utilities-say-they-are-prepared-to-meet-cyber-threats-are-they/572080/
3. Economist (2021), "A cyber-attack exposes risks to America's energy infrastructure", https://www.economist.com/united-states/2021/05/13/a-cyber-attack-exposes-risks-to-americas-energy-infrastructure
4. Simonovich, L. and Beato, F. (2021), "The US pipeline attack shows the energy sector must act now on cybersecurity. Here are 6 ways how", https://www.weforum.org/agenda/2021/05/oil-gas-cybersecurity-ransomware-colonial-pipeline/
5. BBC (2020), "Ransomware-hit US gas pipeline shut for two days", https://www.bbc.com/news/technology-51564905
6. Doan, L. (2021), "Colonial Is Just the Latest Energy Asset Hit by Cyber-Attack", https://www.bloomberg.com/news/articles/2021-05-08/colonial-is-just-the-latest-energy-asset-hit-by-cyberattacks
7. Collins, R. et al. (2018), "Cyberattack Pings Data Systems of At Least Four Gas Networks", https://www.bloomberg.com/news/articles/2018-04-03/day-after-cyber-attack-a-third-gas-pipeline-data-system-shuts
8. Bronk, C. and Tikk-Ringas, E. (2013), "Hack or Attack? Shamoon and the Evolution of Cyber Conflict", *Working Paper*, James A. Baker III Institute for Public Policy, Rice University, https://www.bakerinstitute.org/media/files/Research/dd3345ce/ITP-pub-WorkingPaper-ShamoonCyberConflict-020113.pdf
9. Macola, I. G. (2020), "The five worst cyberattacks against the power industry since 2014", *Power Technology*, https://www.power-technology.com/features/the-five-worst-cyberattacks-against-the-power-industry-since2014/
10. Sanger, D. and Perlroth, N. (2019), "US Escalates Online Attacks on Russia's Power Grid", *New York Times*, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

11. Williams, H. (2016), "Russian hacks into Ukraine power grids a sign of things to come for U.S.?", https://www.cbsnews.com/news/russian-hacks-into-ukraine-power-grids-may-be-a-sign-of-things-to-come/
12. Polityuk, P. et al. (2017), "Ukraine's power outage was a cyber attack: Ukrenergo", *Reuters*, https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA
13. Bergman, R. et al. (2021), "Blackout Hits Iran Nuclear Site in What Appears to Be Israeli Sabotage", https://www.nytimes.com/2021/04/11/world/middleeast/iran-nuclear-natanz.html
14. Findlay, S. and White, E. (2019), "India confirms cyberattack on nuclear power plant", *Financial Times*, https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6
15. McCurry, J. (2014), "South Korean nuclear operator hacked amid cyber-attack fears", *The Guardian*, https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack
16. Energy Community (2019), "Final Report of a study on cybersecurity in the energy sector of the Energy Community", https://www.euneighbours.eu/sites/default/files/publications/2020-02/Blueprint_cyber_122019.pdf
17. Ecopress (2021), "Digital blackout from a cyberattack on Greece's Energy Ministry", *(in Greek)*, https://ecopress.gr/psifiako-blakaout-apo-kyvernoepithesi-chaker-sto-ypen/
18. IPTO (2021), "Upgrade Cybersecurity Resilience of IPTO's Infrastructure", *(in Greek)*, https://www.admie.gr/sites/default/files/promitheies/42115/42115-9-prokiriksi.pdf
19. Hurriyet Daily News (2016), "Major cyber-attack on Turkish Energy Ministry claimed", https://www.hurriyetdailynews.com/major-cyber-attack-on-turkish-energy-ministry-claimed-107981

IENE SEE ENERGY BRIEF MONTHLY ANALYSIS - Issue No. 343 – ISSN:179-9163

Contributed by the IENE Research Team

Monthly Analysis is published by the INSTITUTE OF ENERGY FOR SOUTH-EAST EUROPE (IENE)

3, Alex. Soutsou st. 106 71 Athens, Greece, T: +30-210 3628457, 3640278, F: +30 210 3646144, marketing@iene.gr, www.iene.eu