BRIEFING

Cybersecurity of critical energy infrastructure

SUMMARY

The European Union (EU) has a high level of energy security, enabled by oil and gas reserve stocks, and one of the most reliable electricity grids in the world. However, a number of established and emerging trends pose new challenges to the security of energy supply, notably in the electricity sector. The production, distribution and use of energy is becoming increasingly digitalised and automated, a trend which will further increase with the transformation towards a distributed carbon-neutral energy system and the growth of the 'internet of things', which means that more and more networked devices will be connected to the electricity grid. This provides increased opportunities for malicious actors to carry out attacks on the energy system, notably cyber-attacks, possibly in combination with physical damage and social engineering. It also increases the risk of inadvertent disruption. Hackers are becoming increasingly capable, and are already probing and exploiting vulnerabilities in the energy system, as a number of incidents outside the EU have demonstrated.

The 2008 Directive on European critical infrastructures has been the basis of the EU approach. The EU has recently reinforced its approach to cybersecurity, through legislation, standards and reinforcement of the European Agency for Network and Information Security, which will take on new coordinating and operational roles in cybersecurity. A recent European Commission communication on cybersecurity in the energy system provides guidance, and binding rules for energy system operators are under development in the form of a new network code on cybersecurity.

The April 2019 European Commission recommendation underlines that the cybersecurity of the energy system, and notably the electricity grid, needs a dedicated sectoral approach because of real-time requirements, a mix of advanced and legacy technologies, and the cascading effects of disruptions. Experts see a growing need for improved exchange of knowledge and information, standardisation and certification, development of cybersecurity skills, and regulation.

In this Briefing

EPRS | European Parliamentary Research Service

Author: Gregor Erbach with Jack O'Shea
Members' Research Service

PE 642.274 – October 2019

EN

Current trends in energy systems security

A secure energy system is of critical importance to modern societies. Electricity, gas and oil are not only needed for our day-to-day activities, but also allow other critical infrastructure to function, notably transport, telecommunications, healthcare, finance and defence. The EU has one of the most reliable electricity grids in the world, and possible vulnerabilities have not so far been exploited to disrupt the energy supply on a large scale.

However, elsewhere, energy system vulnerabilities have been exploited, for example in cyber-attacks on Ukrainian electricity grids, attributed to Russian hackers.[1] A 2018 cyber-attack 'likely designed to trigger an industrial accident' in a Saudi petrochemical plant was linked to a Russian scientific institute. According to American energy security experts, malicious actors are suspected to have the capacity to shut down natural gas pipeline operations in the United States (USA) for weeks or even months at a time. Natural disasters such as storms, earthquakes, volcanic eruptions, floods and electromagnetic pulses[2] can also cause serious disruption to energy systems, necessitating more resilient infrastructure.

These instances and others highlight the vulnerabilities of critical energy infrastructure. The ramifications of these emerging threats are numerous: as all sectors of the economy rely on energy to operate, exploiting weaknesses in the grid's critical infrastructure has the potential to initiate a 'cascade effect' that hinders or halts operations in other sectors, such as transport, finance, and healthcare. Disabling the energy grid can provoke civil unrest, disrupt chains of communication, degrade military readiness, and generally impede a government's ability to respond quickly and effectively in a crisis situation. The physical and cybersecurity of critical energy infrastructure is therefore of the utmost importance.

The European energy system is undergoing a fundamental transformation towards a model with a high share of variable distributed renewable energy, flexible demand, energy storage facilities and sector coupling. Moreover, recent energy market reforms facilitate the participation of customers, energy communities, aggregators and new energy and flexibility providers in the market. Electric vehicles are expected to provide services to the electricity grid (vehicle-to-grid technology). All of these trends lead to an increasing digitalisation of the energy system and a growing number of networked devices and control systems. This leads to increased opportunities for cyber-attacks.

Energy flows are increasingly controlled and monitored by networked industrial control systems. The electricity grids are being transformed into smart grids, in which more and more control functions are automated. Industrial control systems are used in the operations of large parts of the electricity and gas grids to control electricity generation, storage and transmission as well as gas storage and pipeline transport. These systems have become a favourite target of hackers. Manipulations of industrial control systems can not only lead to disruption of energy supply, but also to physical damage of equipment[3] and industrial accidents, including explosions and fires. The number of networked devices in the energy system is expected to grow with the spread of the 'industrial internet of things' enabled by the roll-out of 5G wireless communication networks.

On the other hand, electricity use is also becoming 'smart', with internet-connected smart appliances, smart homes, smart electricity and gas meters. These can contribute to the management of the electricity grid and a better alignment of electricity production and demand, but they also present opportunities for cyber-attacks. The same goes for distributed wind and solar electricity generation, energy storage systems, and electric vehicles, which are connected both to the internet and the electricity grid.

The adversaries include cybercriminals, industrial spies, state-sponsored hackers, intelligence agencies and military cyber commands. Their skills and sophistication are continually increasing. To penetrate networks that are physically separated from the internet, they often use social engineering in combination with automated cyber-weapons that find their way to the target systems and autonomously launch a pre-programmed cyber-attack. This creates the additional risk of hitting systems that were not the intended target of the attack.[4]

Notable incidents related to physical and cybersecurity of energy

Reports of hackers penetrating Russian and US power networks, 2019
In March 2019, the US grid regulator NERC reportedly warned that a hacking group with suspected Russian ties was conducting reconnaissance into the networks of American electrical utilities. In June 2019, the *New York Times* reported that American 'code' had been deployed inside many elements of Russia's power network by US military hackers that were targeting Russian power plants. The claims were denied by President Trump and regarded with scepticism by cybersecurity experts.

Cyber-attack on petrochemical plant, Saudi Arabia, August 2017
In August 2017, a sophisticated cyber-attack on a Saudi petrochemical plant was the first known attempt to manipulate an emergency shutdown system. The attack resulted in the plant shutting down, but experts warned that it had the potential to cause a serious industrial accident. Cybersecurity experts attributed the incident to a Russian government-owned laboratory.

Cyber-attacks on Ukrainian power grid, 2015 and 2016
The Ukrainian grid suffered two blackouts as a result of cyber-attacks. In December 2015, hackers penetrated the computer system of a western Ukrainian power utility, and cut off the electricity to some 225 000 people. A year later, in December 2016, a cyber-attack disabled an electricity substation and left customers in parts of Kiev without power for about an hour. Both attacks were attributed to Russian hacker groups. Some security researchers suspect that the second attack was intended to cause physical damage to the components of the Ukrainian electricity grid.

Metcalf sniper attack, California, 2013
In April 2013, attackers physically damaged and disabled the Metcalf substation that supplies electricity to Silicon Valley. In a well-planned night-time operation, they cut communication cables and used rifles to severely damage 17 electricity transformers, resulting in damage worth US$15 million. The attackers were not identified and their motivation is not known.

Baku-Tbilisi-Ceyhan oil pipeline explosion, Turkey, 2008
The Baku-Tbilisi-Ceyhan (BTC) oil pipeline in Turkey experienced a rupture and fire in 2008. The Kurdish Workers Party claimed responsibility for the incident, but later investigations point to a cyber-attack in which the attackers accessed the control system of the pipeline via internet-connected security cameras and gained access to the industrial control systems to raise the pressure in the pipeline, causing it to rupture.

North-eastern blackout, USA and Canada, 2003
Malware may have inadvertently contributed to the 2003 blackout, which left 50 million North Americans without electricity. The blackout happened at a time when the computer worm Blaster affected a large number of computer systems, possibly impeding the timely detection of, and communication about, the initial small power outage, which cascaded to interconnected grids.

The energy system has a number of particularities that necessitate a specialised sectoral approach to cybersecurity, above and beyond cybersecurity standards and measures applied to information technology systems:

- **Real-time requirements**: In an electricity grid, supply and demand must be balanced at any moment, meaning industrial control systems must react within fractions of a second, which leaves no time for sophisticated authentication procedures.[5]
- **Mix of advanced and legacy technologies**: Energy system components have a very long lifespan, of several decades. It is consequently very likely that the grid will be

controlled by a mix of advanced technologies with cybersecurity certification, and older devices which need to be protected in other ways.

- **Cascading effects of disruption**: Due to the interconnected nature of an electricity system, a serious disruption in one part of the grid can also spread to interconnected grids, potentially leading to a blackout over a wide area. This would also affect other services that depend on electricity, notably transport, telecommunications, water supply and finance.

Protection measures against cyber-attacks aim to prevent attackers from gaining access to critical infrastructure, detect any suspicious activity and malware, restore security and remove malware, and repair any damage that has occurred. Measures to prevent attackers from gaining access include regular updating of systems, strong authentication protocols, encryption of communications, private networks that are not connected to the internet, physical protection of networks, security procedures and regular security audits, and training of staff to raise awareness of the risks. Redundant systems help to ensure safe operations in case of an incident.

Analysis of incidents is critical for identifying any security loopholes and establishing the identity or origin of the attackers, a task which is very difficult in a cyber-environment. When malware or an attack is detected, sharing the information in a secure way with authorities and other organisations would help improve overall security, but there is little incentive for information-sharing, and some organisations deliberately hide information about successful attacks for fear of negative publicity. State actors such as secret services or the military even collect information about unpublicised vulnerabilities ('zero day exploits'), in order to use them against their adversaries.

Although a recent survey found that cybersecurity is an important issue for the majority of energy companies, a shortage of staff with specialised skills in cybersecurity is an obstacle to the implementation of cybersecurity technologies and procedures. Moreover, companies tend to under-invest in security measures, which impose a certain cost but an uncertain and hard-to-quantify payoff.

EU policy and legislation

The European programme for critical infrastructure protection (EPCIP), adopted by the Commission in 2006, establishes a framework for action aimed at improving the protection of critical infrastructure across all EU Member States and in all relevant economic sectors – an all-hazards, cross-sectoral approach. The threats addressed by the programme include terrorism, criminal activities, natural disasters and other causes of accidents. Member States hold regular exchanges of information in the frame of the CIP Contact Points meetings.

The key EU law for the protection of critical infrastructure[6] is Council Directive 2008/114/EC on critical European infrastructures. It establishes procedures for identifying and designating European critical infrastructures (ECI) and introduces a common approach for assessing their protection and the need to improve it. The Directive applies only to the energy and transport sectors. It requires owners or operators of designated ECI to prepare advanced business continuity plans (operator security plans) and to nominate Security Liaison Officers that act as contact points to the national authority responsible for critical infrastructure protection.

In June 2019, the Commission published an evaluation of the Critical Infrastructure Directive (2008), which found that the Directive's relevance has diminished in the light of new and evolving challenges brought about by technological, economic, social, political and environmental developments. It concludes that the Directive has been partially effective, but failed to establish a common approach to the assessment of critical infrastructure protection measures. Options identified for a future review of the Directive include a more systems-focused approach and better alignment with other relevant EU legislation.

In February 2013, the Commission issued a cybersecurity strategy that outlined the EU's vision for building cybersecurity capabilities.

Network and Information Systems (NIS) Directive: Directive (EU) 2016/1148, a key deliverable of the cybersecurity strategy, sets rules (transposed into national law by May 2018) that form the basis for the current EU cybersecurity regime. The NIS Directive requires the designation of national competent authorities, the creation of computer-security incident response teams (CSIRT), and the adoption of national cybersecurity strategies. It also obliges essential services providers and digital service providers to take the appropriate security measures and to notify the relevant national authorities about serious incidents. National competent authorities monitor the application of the Directive by assessing the cybersecurity policies of key providers and by participating in the work of the NIS cooperation group, which comprises competent authorities as well as representatives of the European Commission and the European Union Agency for Network and Information Security (ENISA). In June 2018, the group created a work stream dedicated to energy.

Cybersecurity Act: Regulation (EU) 2019/881 (Cybersecurity Act), which is part of the 2017 cybersecurity package and entered into force in June 2019, aims to strengthen the EU's response to cyber-attacks, improve cyber-resilience and increase trust in the digital single market. The Act empowers ENISA – now referred to as the European Union Agency for Cybersecurity – to improve coordination and cooperation in cybersecurity across EU Member States and EU institutions, agencies and bodies. It establishes an EU cybersecurity certification framework for the development of tailored certification schemes for specific categories of information and communication technology products, processes and services. Companies will need to certify their products, processes and services only once to obtain certificates that are valid across the EU. The Act provides ENISA with more financial and human resources to carry out its new tasks and also addresses the issue of legacy infrastructure – that is, older technology with a lifespan of 30-60 years, designed before cybersecurity concerns existed.

Commission Recommendation on energy cybersecurity: In April 2019, the Commission issued Recommendation (EU) 2019/553, which contains guidelines that Member States and key stakeholders (particularly energy grid operators) should take into account when making decisions about infrastructure. These measures include cybersecurity risk analysis and preparedness, in particular for legacy systems, updating software and hardware, and establishing an automated monitoring capability for security events in legacy environments.

Security of Gas Supply Regulation: Regulation (EU) 2017/1938 deals with gas supply shortages caused by a number of risk factors, including cyber-attacks, war, terrorism and sabotage. It sets out rules for regional risk assessments and emergency planning, and introduces a mechanism for mutual assistance in the event of a severe gas supply crisis, based on the principle of solidarity.

Electricity Risk Preparedness Regulation: Regulation (EU) 2019/941 is focused specifically on crisis prevention and crisis management in the electricity sector. It envisages the development of common methods to assess risks to the security of electricity supply, including risks of cyber-attacks; common rules for managing crisis situations and a common framework for better evaluation and monitoring of electricity supply security.

The European Commission organises regular information-sharing events, such as the high-level event on cybersecurity in the energy sector, held on 9 July 2019.

Ongoing developments

Network code on energy cybersecurity: The recast of the Electricity Regulation (Regulation (EU) 2019/943) gives the Commission a mandate to develop a network code[7] for cybersecurity. The Smart Grids Task Force has been doing preparatory work since 2017, and released its second interim report in July 2018. The report recommends setting up an early warning system for the energy sector in Europe, cross-border and cross-organisation risk management, minimum security requirements for critical infrastructure components, a minimum protection level for energy system operators, a European energy cybersecurity maturity framework and supply chain risk management.

Expert and stakeholder involvement

Cybersecurity in the energy sector involves several key stakeholder organisations, and efforts have been made in recent years to incorporate these actors into forums to share best practices and establish uniform cybersecurity norms. Working groups like the Smart Grids Task Force, the Electricity Coordination Group (ECG), and the European Energy – Information Sharing & Analysis Centre (EE-ISAC), act as forums for utilities, agencies, and other relevant actors to build working relationships and exchange best practices for cybersecurity. The Critical Energy Infrastructure Security Stakeholders Group (CEIS-SG) has been established as a think-tank and information exchange forum to guide and coordinate efforts to improve the security and resilience of critical energy infrastructure (CEI). It is supported by the EU through the research framework programme Horizon 2020 (project Defender). CEIS-SG aims to define a roadmap for next generation CEI security by design and by default, develop security certifications and to promote best practices at pan-European level.

Approaches in other jurisdictions

United States of America

In the United States, the first significant piece of legislation to address the growing challenge of cybersecurity in the energy sector was the 2005 Energy Policy Act. Signed into law less than two years after the North-east blackout of 2003 left 50 million North Americans without power, the act granted the Federal Energy Regulatory Commission (FERC) the ability to appoint an Electric Reliability Organization (ERO) that would develop and enforce mandatory reliability standards for all bulk power electric utilities in the country. The North American Electric Reliability Corporation (NERC), a private non-profit organisation, was designated as the ERO for the United States and several Canadian provinces in 2006. The NERC is responsible for developing a list of critical infrastructure protection standards (NERC-CIPs), which are delivered to the FERC for review. Of the eleven CIPs currently subject to enforcement, ten are dedicated to cybersecurity standards and one relates to the physical security of energy grids.

Addressing infrastructures for electricity production and transmission, NERC-CIPs, 'are among the most detailed and comprehensive cybersecurity standards in the world'. These standards can also be updated rapidly when necessary, adjusting effectively to the fluctuating cybersecurity environment. In most instances, however, NERC does not specify how utilities should meet the standards, instead mandating that utilities exercise 'reasonable business judgement'.

Government agencies in the USA are adopting a holistic approach to the problem of energy cybersecurity, partnering with industry and local officials to counter emerging threats. The new Office of Cybersecurity, Energy Security, and Emergency Response (CESER), for example, is designed to lead the Department of Energy's coordinated response to disruptions by partnering with the National Laboratory system, private sector coordinating organisations, and state and local governments. The cybersecurity risk information-sharing program (CRISP) is a voluntary public-private partnership primarily funded by industry. Exercises like Clear Path VI – an annual NERC-led simulation of a cyber-attack on energy infrastructure across North America – can also help develop interagency coordination during crises.

Australia

The Australian government has established the Australian Cyber Security Centre (ACSC) with Joint Cyber Security Centres (JCSCs) positioned around the country in state capitals. Throughout 2019, the ACSC will oversee a nationwide programme of cyber resilience and response activities for the electricity industry and for government agencies that have an energy and cybersecurity role, including information exchange and training activities. These activities culminate in a two-day functional exercise for Australia's electricity industry in November 2019.

Outlook

The security and resilience of the European energy system will remain a critical issue in the foreseeable future. A number of current trends will heighten the need for strong socio-cyber-physical security measures and policies, notably in the electricity sector.

Digitalisation and automation: This trend affects the energy system through the move towards a smart grid with more and more networked grid components, from electricity generators, through transmission and distribution networks to smart meters in the home. A growing number of electricity-consuming devices in households and industry will be connected on the internet of things, enabled by the rollout of 5G telecommunications networks. All of these devices present potential opportunities for attacks or inadvertent disruption.

Sustainable energy: With the objective of achieving a climate-neutral energy system, the electricity system will be increasingly decentralised (distributed wind, solar and hydropower installations). It will also be increasingly interconnected in order to balance variable renewable generation between regions. In addition electric vehicles, storage, smart appliances and flexible industrial demand all lead to a dramatic increase of potentially vulnerable networked devices on the electricity grid.

Market reform and consumer empowerment: Reforms of the electricity market allow new actors to participate. This includes energy companies, aggregators, energy communities and individual citizens. Many of these will not have adequate cybersecurity skills and therefore need to rely on certified equipment, software and service providers.

Capabilities of adversaries: Hackers' skills and toolkits are constantly evolving. Potential adversaries include cybercriminals, government-sponsored hackers, terrorist groups and military cyber-commands. Automated attack tools have the potential to spread in the network and cause damage beyond the intended target. Artificial intelligence has the potential to boost the capabilities of attackers as well as defenders, and can prove to be a critical advantage.

Skills and investment incentives: With the increasing need for cybersecurity skills, the current shortage of skilled personnel is likely to persist. Information and knowledge sharing, as well as automation, will be instrumental in making the best use of the available skills base. Moreover, the market does not sufficiently incentivise investment in security and resilience, meaning regulation and public investments may be needed.

With these rapid evolutions in the energy system and in information/communication technologies, energy system cybersecurity is expected to remain a priority on the EU agenda in the coming years. There will be a need to continually adapt security measures and policies to continually evolving threats and to strengthen energy systems' resilience in the face of deliberate attacks and inadvertent disruption. Adequate investment in cybersecurity, development of relevant skills, and information and knowledge sharing are among the key prerequisites for ensuring a secure and resilient energy supply.

Responding to the emerging threat of equipment manipulated by the manufacturer, the European Parliament adopted a resolution in March 2019, calling for action at EU level on the security risks linked to China's dominating role as a supplier of 5G telecommunications equipment, which is likely to play a key enabling role in smart grids and a distributed, sustainable energy system.

MAIN REFERENCES

Barichella A., Cybersecurity in the energy sector: a comparative analysis between Europe and the United States, Études de l'Ifri, February 2018.

Schneier B., *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*, Norton, 2018.

Negreiro M., ENISA and a new cybersecurity act, European Parliament, EPRS, July 2019.

Cyber Security Strategy for the Energy Sector, Policy Department for Economic and Scientific Policy, European Parliament, 2016.

Livingston S., et al., Managing cyber risk in the electric power sector, Deloitte, 2018

Report on recommendations for the European Commission on Implementation of a Network Code on Cybersecurity, Smart Grids Task Force, July 2018.

Kasper A., and Antonov A., Towards Conceptualizing EU Cybersecurity Law, ZEI Discussion Paper C 253, 2019.

Cyber Security in the Energy Sector, Energy Expert Cyber Security Platform, February 2017.

ENDNOTES

[1] In this document, the term 'hackers' refers to individuals or groups that break into computer and industrial control systems to take control, or design software tools (malware) to perform such tasks.

[2] Strong electro-magnetic pulses, originating from solar eruptions or from EMP weapons, can cause considerable damage to the electricity grid (especially transformers) and electronic devices. Experts warn that a solar storm like the 1859 Carrington event could cause catastrophic damage to the electricity grid and to digital equipment. In March 2019, US President Trump issued an executive order on coordinating national resilience to electromagnetic pulses.

[3] An early example of an attack on industrial control systems is the Stuxnet computer worm (malware) that was probably brought into an Iranian nuclear plant in 2009 on an infected USB stick and caused significant damage to industrial centrifuges used for enrichment of uranium.

[4] In 2017, a malware supposedly targeted at Ukrainian companies, severely disrupted the global operations of A. P. Møller-Maersk, one of the world's largest shipping companies.

[5] In conventional electricity grids, large rotating machines such as generators and industrial motors provide enough inertia to compensate for short-term fluctuations. In a modern, increasingly digitalised system, these are displaced by generation technologies like solar panels and electronic devices as energy consumers, which provide no such stabilising function.

[6] The Directive defines critical infrastructure as 'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions'.

[7] Network codes are binding rules for the EU energy system developed by the Agency for the Cooperation of Energy Regulators (ACER) in cooperation with the European networks of transmission and distribution operators, after consultation with stakeholders. They are approved by the EU Member States in a comitology procedure and adopted by the Commission as implementing regulations.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Photo credits: © urbans78 / Fotolia.

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)