STORMSHIELD

From 2015 to tomorrow:

cyber-intrusions in electrical grids

White paper



Executive Summary

If you wanted to harm a country, which targets would you attack first? One answer comes to mind immediately: its power production grids.

And with good reason: today, nothing works without electricity. From our industries, to tertiary companies, to cities (whether or not they are already *smart*) to our households. Well-conducted cyberattacks, to the point of paralysing a power plant or even causing a *blackout*, can also have major impact on populations and states. Being able to inflict damage on power grids means having a powerful means of political and financial destabilisation.

Cybercriminals have understand this and have not failed, in recent decades, to concentrate on energy systems. The Observatoire de l'Industrie Électrique has thus compiled a list of over twenty major cyberattacks concentrated in this sector in various countries since 1982, with a strong acceleration after 2010. And that trend has been confirmed over the past five years – both at the level of information technology (IT) or operational technology (OT) networks.

The digitization and Internet connections from which power grids have benefited in recent years have largely contributed to their exposure to cyber threats. Such operational systems, developed with the constant aim of ensuring the security of their operation, were not designed to integrate cybersecurity risks, however – despite regulatory advances in this sense with the NERC-CIP standard and the EU's NIS directive. With the extraordinary deployment of information and communications technologies (ICT), power grids are now smart. Capable of processing a considerable volume of data, they also rely on forecasting and modelling tools, as well as on storage technologies. Result: they now refine their management of electricity flows in real time, based on information transmitted between suppliers and consumers. But that optimisation of power distribution carries a weakness: involuntarily opening new access doors for cybercriminals within the electrical power management system.

Faced with this evolving, contagious threat, many states are mobilising at every level (national and international alike). Some countries have not hesitated to make IT security a national priority, often as a direct response to attacks suffered, or after becoming aware of the risks.

In parallel, private economic actors have also organised themselves in order to effectively protect against cybercriminality. To help them, companies like Stormshield specialise in the security of critical infrastructures, sensitive data, and operational environments, by designing complete security solutions.

For Stormshield, developing this work, dedicated to the evolution of cyberattacks on power grids since 2015 is a natural extension of what represents its core business: analysing malicious cyberattacks, anticipating the risks to come, and proposing solutions

I.
2015-2020: retrospective of the principal cyberattacks in the electrical world

1. Retrospective analysis
2. New practices in threats

II.
Electrical grids: a choice target

1. Industrial reasons
2. Technical reasons

III.
The nature of the threat

1. The players in cyberspace
2. The principal targets of cyber threats
3. Operating methods
4. Human shortcomings

IV.
Protection strategies

1. Regulatory aspects
    - In France
    - In Europe
    - In the US
2. Standards
3. Electrical infrastructure protection in practice

V.
And what will there be tomorrow?

1. Toward accelerating geopolitical tensions
2. Is Europe ready to deal with this?
3. Are companies in working order?

I. 2015-2020: retrospective of the principal cyberattacks in the electrical world

Over the past five years, a number of cyberattacks have impacted the world of electrical energy and, for some, triggered awareness and changes in terms of cybersecurity. Focus on their operating methods and impacts.





Target: a portion of the Ukrainian power grid (Ivano-Frankivsk, in the western part of the country)

Incident date: 23 December 2015.

Damage caused: a power plant went off-line for several hours, plunging 80,000 people into darkness, followed by several weeks of disruptions before a return to normal.

Operating method: the attackers lured their initial targets through a spearphishing campaign. That made it possible to introduce a Trojan horse, dubbed BlackEnergy, into the Ukrainian plant, combined with a "KillDisk" module capable of erasing data and destroying hard drives. Once the computers were infected and controlled, the attack was expanded to the supervisory control and data acquisition system. In parallel, the cybercriminals launched a DDoS attack on the emergency call centres, thus rendering them inaccessible to the people affected by the blackout.

Distinctive feature of this cyberattack: it was the first cyberattack to trigger a full, long-term power outage. According to Tarik Zeroual, Global Account Manager for Stormshield, "*other attacks had previously targeted energy sector infrastructures, particularly the oil & gas industry, but none had such an impact on the population. Some analysts consider it a textbook case of industrial sabotage*".





MALWARE



SCANNING SYSTEM

Target: the power grid serving the capital of Ukraine (Kiev)

Incident date: December 2016.

Damage caused: partial power outage in Kiev for one hour.

Operating method: to obtain this result, the cyberattackers used malware dubbed Industroyer or CrashOverride. In practice, they used backdoors to access the PCs of power grid administrators. Next, they installed remote control and network scanning modules, while erasing system files on the infected PCs. Objective: removing any traces of their intrusion (data wiper).

Distinctive feature of this cyberattack: Industroyer was specially designed to attack power grids, particularly Ukrainian ones. But it was next observed that the malware adapted to European, Asian, or Middle Eastern sites. More worrying, cybersecurity researchers made it clear that it was able to infect other major targets. In fact, in order to reach the various installations of the power grid, it used their vulnerable communications protocols which were also used in various infrastructures of water utilities and highway traffic networks. Furthermore, according to some experts, the malware was not used to its maximum potential. Their hypothesis? Since with Industroyer, the cyberattackers could move about using communications protocols without knowing them, they were able to reach the circuit breakers of one or more transformers and thus trigger a blackout. But they did not do that. Could this operation be reduced to a simple show of force? In any case, it was compared to Stuxnet and represented the most powerful threat to industrial control systems since the infamous cyberattack on the Natanx nuclear power plant in Iran.





PHISHING

Target: Burlington Electric Department, a power provider in the state of Vermont (USA)

Incident date: December 2016.

Damage caused: none. Despite the introduction of malware into one of the laptop computers of the Vermont power company, not connected to the operational network, the attack was without consequence. But its objective probably was to serve as a vulnerability test for a subsequent operation.

Operating method: the cyberattackers probably used phishing to obtain the passwords from employees of the US power grid supplier in order to penetrate it.

Distinctive feature of this cyberattack: the Americans did not take this threat lightly, considering that the cybercriminals had attempted to gain access to suppliers in order to potentially manipulate the power grid and shut it off in the middle of winter. Following that attack, the Department of Energy step up the protections for electrical and gas networks. This was followed, in 11 May 2017 by the issuance of an Executive Order by President Trump in order to protect vital US infrastructures against cyberattacks.

PASSWORD

Target: the US electrical power grid (as well as oil & gas companies)

Incident date: from 2019 to 2020.

Damage caused: vast industrial espionage operation.

Operating method: in November 2019, Microsoft detected suspected large-scale password spraying attacks on US electricity companies. More discrete than a brute force attack, this technique consists of guessing low-security passwords common to a maximum number of accounts.

Distinctive feature of this cyberattack: it took place in late 2019 and early 2020, at a time of elevated tensions between the United States and Iran. Even if, according to experts, the techniques used were not sophisticated enough to access the OT infrastructures of the power grids, they were sophisticated enough to affect their IT systems, attempt to find weaknesses, paralyse them, or open the way to subsequent destructive attacks.

MALWARE

Target: a French wind farm connected to the electrical distribution network managed by Enedis

Incident date: January 2018.

Damage caused: attempted intrusion thwarted before it could cause any damage.

Operating method: without further clarification on its introduction, a sophisticated malware (a BlackEnergy variant) was discovered at a French wind farm.

Distinctive feature of this cyberattack: the French authorities fully appreciated the significance of this operation, which was considered an act of espionage, or even sabotage. Their hypothesis: the cybercriminals had intended to penetrate further into the power distribution network managed by Enedis, in order to install dormant implants on it. Such implants would have made it possible to significantly impact the functioning of the electrical grid.

PHISHING RANSOM-WARE

Target: the internal network of Elexon, a crucial English company in the British electricity supply chain.

Incident date: May 2020.

Damage caused: infection of the internal network, blocking the company's professional email addresses and laptop computers.

Operating method: Following a phishing operation against an employee working remotely, the cybercriminals used a software program to encrypt the company's data. That program was ransomware (known as Sodinokibi and REvil). While waiting to restore from backups and finish analysing its system, Elexon found itself paralysed. Experts estimate that the cyberattack was favoured by the VPN used by the company, which had been out of date for several months.

Distinctive feature of this cyberattack: the cybercriminals targeted an important actor in the electricity supply chain, but one with less oversight than the National Grid Agency.

New practices in threats

As the years have gone by, cyber threats on electrical grids have grown more sophisticated. While the electrical energy world may sometimes be a target of independent hackers, it is most often exposed to precise threats, meticulously prepared by organized groups of cyberattackers. They are showing increasing patience and sophistication in the deployment of their attacks and analysing all opportunities, even indirect ones. And some operations would probably never have seen the light of day without the support of states, whose motivations we will examine later (see *II Electrical grids: a choice target*).

Cybercriminals are aware that, by "simply" targeting the IT networks of an electricity company, they can cause significant damage: to distribution grids, of course, but also to a company's "business tools" (as in the case with Elexon), in order to block its commercial interfaces and thus paralyse its business. Often less well-protected, the vendors and service providers of the actual target of cyber criminals may thus unwittingly serve as entry points for a cyberattack (like the attack on Elexon, which is how the cybercriminals in the Dragonfly group managed to regularly penetrate the United States power grid between 2015 and 2018, and perhaps earlier).

More rarely, highly-targeted attacks manage to reach their targets' surveillance (SCADA) and control (ICS) systems. In the case of the Industroyer malware used in Ukraine in 2016, the cybercriminals provided it with communications modules capable of connecting to the power grid control stations on the IT networks of national and regional operators. Once infiltrated, the malware was able to communicate directly with the application programming interfaces (API) of the power grids, enabling it to steal data and perform acts of sabotage, like cutting the communications between the control stations and electrical substations and thus depriving operators of information on the status of the grid.



II. Electrical grids: a choice target

Nuclear installations and electricity distribution grids represent a country's top critical infrastructures and sensitive operational environments. Damaging their integrity means considerably affecting economic security and public order. This explains why cybercriminals are intensifying their activities in order to exploit weaknesses in power grids, which are within their reach more than ever before.

1. Industrial reasons

Essential since the second half of the 20th century, electricity plays a central role in the functioning of our countries' economy. In a world where nearly all production resources and exchanges are based entirely on electricity, cybercriminals have well understood that they were able to cause considerable damage if they managed to interfere with its generation and distribution. Electrical grids therefore are especially at risk because they represent strong levers for action, exploitable remotely.

According to the Observatoire de l'Industrie Électrique, a real change began in 2017. Industrial and energy systems, of vital importance, and transport systems, became the target of cyberattacks initiated by states or terrorist groups. "*Cyberdefense and cyberattacks are progressively becoming essential as new strategic weapons aimed especially at the functioning of states*", the Observatoire emphasizes. Because targeting an electrical infrastructure can cause more significant impacts than directly targeting a state, but it is also an easier objective to achieve than major government sites, which are better protected. In fact, power grids have specific weaknesses that cybercriminals do not fail to exploit (see *part 2 Technical reasons*).

Moreover, employing a cyberattack makes it possible to destabilize a country while remaining under cover, with less risk of conflict than opting for armed force, since it is so difficult to determine the perpetrator – and even more so to determine its actual backer. Officially attributing a cyberattack to another state also involves sensitive diplomatic considerations, which are far from trivial. In March 2019, Venezuelan President Nicolás Maduro accused the United States of being responsible for electricity and communications outages in the country.

But not all states have an arsenal for retaliating, not necessarily having the technical resources to assert themselves in cyberspace, now a zone for latent geopolitical attacks. As often is the case in cybersecurity, it will often be the same names coming back in advanced scenarios.

The consequences of a cyberattack in practice

Attacking power plant networks can generate major material damage (such as disrupting centrifuges resulting in their physical destruction), hampering the economy of a region and considerably disrupting the daily life of its citizens.

In a 2011 report, the German *Office of Technology Assessment* contemplated what would be the consequences of a long-term power outage. Once the electrical generators are out of service (following a diesel shortage), and telecommunications are reduced to the bare minimum (informing citizens and functioning of the army, hospitals, police, and government), public services and companies would be paralysed. Water and food supplies (disruption of cold chain) would quickly become problematic; transport would no longer function, in addition to hospitals, causing generalised chaos. It would take several months to return to normal.

1 trillion

dollars

The cost of a power outage in the United States

In 2015, the insurer Lloyd's, along with the University of Cambridge's *Centre for Risk Studies*, imagined the financial implications of a major cyberattack, using the US electrical grid as an example. Thus, the cost of a power outage plunging 15 US states (i.e., 93 million people) into darkness would come to 243 billion dollars, or as much as one trillion dollars in the extreme version of the scenario. According to Tom Bolt, director of performance management for Lloyd's, this "*scenario shows the huge impact and havoc that could result from a major cyberattack on the US. The reality is that the modern, digital, and interconnected world creates the conditions for significant damage, and we know there are hostile actors with the skills and desire to cause harm*".

2. Technical reasons

Along with their vital role in the functioning of a country, electrical infrastructures are also targeted by cybercriminals due to their technical vulnerabilities. And human ones.

Interconnected networks: a gateway to the electrical grid

Nuclear installations in particular – and OT networks of the energy industry in general – were usually designed to operate without a direct connection to the Internet (because most of them date to before its use or because they simply didn't need it in the past). However, we have seen that cyberattacks target traditional so-called "IT" systems of power grids, which are connected and therefore open the way to cybercrime. On the one hand, they seek to paralyse the electricity supply, e.g., by infecting the management system where logistical orders are managed using IT systems.

On the other hand, cybercriminals can, using the same IT systems, attempt to impact the OT networks. "*Even though operational networks were not initially connected to IT systems*", Tarik Zeroual, Global Account Manager with Stormshield, clarifies, "*the two types of systems have become less compartmentalized over time*". Particularly due to the digitisation of all processes and the processing of data flows. This

is the flipside of the effectiveness and immediacy offered by the interconnection of electrical operational networks using IT networks. The pooling of systems constitutes significant vulnerability points because, once introduced into a portion of the network, a virus can spread dreadfully in the case of faulty segmentation.

Thus, one of the major vulnerabilities of energy systems resides in the fact that they were designed when the cyber risk did not exist. From compartmentalized, hard-to-access industrial networks, they have gone in just a few decades to open systems, run by interconnected technologies.

Internet of Things: increased cyber risks

The fairly revolutionary deployment of the *Internet of Things* (IoT), particularly in the industrial environment (IIoT - *Industrial Internet of Things*) has expanded the attack surface for cyber criminals by increasing the number of entry points for exploiting vulnerabilities within networks, and by giving them access to targets previously beyond reach.

In 2014, at the *Black Hat Europe* conference, two Spanish researchers showed that they could take control remotely of smart meters deployed in Spain and divert their features; e.g., to cut off a neighbour's electricity or collect data from other meters. But, according to the Observatoire de l'Industrie Électrique, the main danger results from the invalidation of sources "*which renders connected objects inoperable or cuts off access for the manager to the control of systems*".

We have noted that functional teams are often unaware of basic cybersecurity rules.

Old equipment: a vulnerability that is hard to correct

OT networks have a very long service life, generally over 25 years. This is the case for electrical infrastructures, designed to work for over 50 years. Most of them are based on obsolete technologies and are therefore highly vulnerable in terms of security.

Further adding to their fragility, electrical systems often use turnkey systems, which were not designed to receive patches. Any modification made to this type of system will require time (and particularly the shutdown of certain equipment, therefore potentially power production), as well as a major financial investment. And since the systems used have been on the market for a while, they have potentially been studied by cybercriminals.

The human being: a link in a fallible system

The biggest breach in the cyberdefenses of OT and IT systems is located "*between the chair and the keyboard*": it's the result of the user. So much so, that, as Vincent Nicaise, Industrial Partnership and Ecosystem Manager for Stormshield points out, "*generally, in industrial companies, we see that the functional teams have little awareness about basic cybersecurity rules, unlike IT staff who, as the years go by, have been trained and seen a number of security rules imposed on them (using complex passwords changed regularly, caution when opening emails, etc.). In OT, operators may sometimes use the same passwords or use personal USB drives for professional purposes*".

Renewable energies: more exposed?

More recent than networks dedicated to the development of fossil energies, renewable energy production equipment might seem less vulnerable at first, since they were designed with connectivity in mind. In fact, in order to manage the intermittent yield of the wind and sun, they have been equipped with specific digital technologies in order to run them remotely and thus regulate the production of electricity to be injected into the grid and stored.

But we are forced to note that many manufacturers have not been made aware of the risks of a cyberattack on their equipment. Which did not escape the cybercriminals of the Dragonfly group, which apparently managed to introduce malware into several renewable energy companies in the United States and Europe in 2013. Managing to exploit their weaknesses, the intruders were able to reach the industrial control systems proper. While their objective was to spy on their targets, they proved that they were able to take physical control of the infrastructures. In 2017, a cybersecurity researcher demonstrated that inverters manufactured by the German company, SMA, connected to the Internet and used to transfer direct current (DC) from photovoltaic panels to alternating current (AC), presented some twenty vulnerabilities. Among his scenarios, he mentioned the possibility of taking control of the equipment remotely and stopping the flows of electricity. Luckily, the European energy transition policies are increasingly including cybersecurity issues. In 2016, for example, the European Commission recommended, in its "*Clean Energy for All Europeans legislative proposals*", identifying the potential cyber-risks for each new green technology. Some experts have drawn attention to the importance of enhancing cybersecurity requirements at all levels of energy production systems, including homes.

III. The nature of the threat

Over the past few decades, the attacks suffered by power installations have probably all occurred from outside and digitally. In fact, the last three instances of sabotage conducted internally (usually by employees) go back to 1992 (Ignalina nuclear power plant in Lithuania; Refinery in Richmond, CA in the US) and 1999 (gas pipelines belonging to Gazprom in Russia). Since then, criminal attacks have been initiated through electronic viruses or worms introduced from outside.

1. The players in cyberspace

Through our retrospective, we have seen the outlines and processes of individuals acting covertly to launch cyberattacks on electrical infrastructures. Most often, such operations (such as those conducted using Stuxnet or BlackEnergy malware) are unofficially ordered by state actors and have significant human and financial resources, given the political stakes represented by such energy industry targets. More rarely, such cyberattacks may be the work of isolated cybercriminals, with modest resources.

According to an analysis of the cyber world as a whole, conducted by analysts with Thales and Verint, four major categories of attackers are acting ruthlessly on the Internet and can be differentiated based on their motivations and their objectives. Thus, the sixty-some major groups of attackers analysed can be broken down as follows:

- **49% of cybercriminals are state-sponsored groups** usually with the purpose of stealing sensitive data from targets of geopolitical interest and/or essential infrastructure providers. They are behind most operations deemed *Advanced Persistent Threats* (or APT). Such cyberattacks, meticulously prepared and targeted, make it possible to infiltrate a network and remain undetected for a long period, in order to monitor its activities.

- **26% of cybercriminals are "hacktivists"**, driven by ideological motivations (community, religious, political, etc.). To achieve their goals, they mainly use DDoS attacks or vandalizing websites (by damaging or erasing information or replacing it with content serving their objective of proselytizing or disinformation).

- **20% of cyberattackers are motivated solely by financial gain.** Without any actual direct connection to the energy sector, they like to use ransomware or attack places where cryptocurrency is exchanged, as well as video game virtual currency.

- **5% of groups analysed are cyber-terrorists.** They seek to recruit new members or destroy data (e.g., using wipers) or infrastructures (by erasing data or using intrusion tools often accessible to the public online).

While these percentages may change slightly if applied to the electricity sector alone, it is nevertheless exposed to these different actors and different threats – whether state actors, hactivists, terrorists, or even financial threats using ransomware attacks. The knowledge of such a

panorama thus enables electricity sector actors to be aware of the risks and thus prepare to face such potential cyberattacks.

Review of the malware market: from custom to a modifiable version

The first sophisticated cyberattacks were designed based on custom malware. The Stuxnet work, discovered in 2010, was specially designed to disrupt the frequency converter controlling the speed of the centrifuge motors for the Natanz nuclear plant: thus it was able to slow and accelerate them repeatedly in order to destroy them.

But an analysis of more recent attacks shows that the current trend is no longer to develop their own "*tools*", but to buy malware on the Dark Web, reused as-is or modified to suit their needs (Industroyer is a good example, since it includes a toolbox that requires no knowledge of the industrial protocols used in the infrastructure).

Thus, even top-notch cybercriminals, supported by states, do not necessarily create their own malware. Many of them use viruses developed by other specialised cybercriminals and include them in their cyberattack strategy.

2. The principal targets of cyber threats

Cybercriminals sell their services for all sorts of causes, when they are not acting on behalf of their own interests. Thus, there are three types of objective that may motivate a cyberattack.

- **Military or terrorist sabotage based on political or even geopolitical reasons**, and which seeks to interrupt the availability of a service or system.
- **Espionage, data theft, or blackmail**, based on financial or economic motivations, for the purpose of exfiltrating information or monitoring an activity.
- **Methods testing or notoriety campaign** aimed at altering information or processes.

3. Operating methods

Since this occurs through the principal cyberattacks that we have presented, electricity infrastructures may be threatened by targeted attacks (like the one that struck in Ukraine with the Industroyer malware). These are designed to infiltrate a specific type of equipment and have therefore used custom, sometimes unheard-of methods (revealing a *Zero-day* vulnerability, i.e., an IT weakness with no known patch). Often planned in detail, such cyberoperations require above-average resources and high technical skills. Groups of cybercriminals associated with Advanced Persistent Threats (APT) usually operate in this way.

For all that, electrical installations are often the subject of attacks that were not specially "calibrated" to the energy sector, but to affect the

IT systems of public or private organisations, via the Internet or email. Thus, they may indirectly affect some elements of OT networks, such as *Industrial Control Systems* (ICS). This was the case of the worldwide cyberattack launched with the NotPetya malware in June 2017: when the cybercriminals of the Lazarus group managed to infect thousands of computers around the world, including the equipment of Ukrainian, Russian, American, and French companies (particularly including SNCF, Auchan, and Saint-Gobain). As collateral damage, the attack took out the radioactivity measurement equipment for an Ukrainian nuclear plant.

4. Human shortcomings

Targeting the employees of a structure remains the easiest gateway to open. Thus, cybercriminals are counting on human error, inattention, or intervention to inject their malware into networks, despite their being protected by defence mechanisms that the cybercriminals often would not be able to get around otherwise. Some techniques used have very evocative names, such as *phishing* or *water holing*, which we will discuss a bit later. The objective is to trap an employee of the target and lead them to unwittingly commit the action that will open up access to the network.

An infected removable storage device (like a flash drive), sharing login credentials via email, logging into the company network via public WiFi network: some ways of accessing the targeted network are particularly elaborate, but remain very effective. In the words of one employee working at an industrial installation, the easiest way to introduce malware there would be to "*drop some infected flash drives in the company parking lot. Then, just wait for an employee to use one at the site*". In other cases, the cybercriminals demonstrate having a lot of imagination. In 2015, a group of cybercriminals managed to arouse the interest of some employees at a power plant using an email claiming to be from the Ukrainian parliament, asking them to open an infected Microsoft Office document (containing the BlackEnergy malware; see the first cyberattack in our retrospective). As for the Dragonfly group, in 2017 it managed to infiltrate the English power grids by imitating a web platform used by employees of the target in order to obtain access codes.

Like no other company having an OT network, companies in the world of electrical power are aware of a series of cyberattack techniques. A quick overview.



PHISHING

Despite being well-known to the public, **phishing campaigns** remain in common use by cybercriminals. They consist of sending mass emails, generally not personalised, in order to receive a response from the recipient. And extract information from them about themself or their company, or to get them to click on the attachments they contain.



WATERING HOLE

The falsified website itself represents another type of trap: **the watering hole.** Like a predator waiting in ambush at a watering hole that they know is frequented by their prey, cybercriminals direct their targets to and/or await them at a website that they have compromised. In this way, they obtain essential information (like login IDs and passwords) to then continue their cyberattack on the target company, or downloading onto the computer of the site user without their knowledge.



SPEAR PHISHING

Spearphishing, more sophisticated, it is much more difficult to detect because it contains information on its recipient (contact information, job title, interests, etc.). The sender may pretend to be a person known to the recipient and often pressures them to act urgently to prevent an irreparable situation (closure of an account, significant losses, etc.) giving them little time for reflection. Like phishing, spearphishing may contain infected attachments or a link to an imposter website.



DRIVE BY DOWNLOAD

Drive by Download attacks are frequently used to spread malware. In practice, cybercriminals target a poorly-secured website and insert a malicious script in the HTTP or PHP code of one of its pages, to insert malware directly on the computer of a visitor to the page. The user does not need to click on a download link or open an attachment in order to become infected. This is how the NotPetya virus attack was launched in 2017, through the update of a compatibility program.

IV. Protective strategies

The stakes associated with sensitive energy infrastructures have made public authorities aware that it was necessary to establish a framework regulating their cybersecurity. Various standards have also been developed in order to provide guidelines on the subject. A brief, comprehensive overview.

1. Regulatory aspects

In France

France laid the foundations of its cybersecurity policy with the **Military Programming Act (LPM), adopted in 2013.** This law required protective measures and strict obligations for Operators of Vital Importance (OIV), including electrical infrastructures. It encourages such operators to strengthen the critical IT systems they operate: IT Systems of Vital Importance (SIIV). In August 2016, France issued **industry-wide orders for its OIVs**, one of which is applicable to electrical energy supply activities. It establishes security rules, both organisational and technical, for OIVs in the sector, applicable to SIIVs, as well as the modalities for identifying SIIVs and for reporting security incidents affecting them.

In Europe

Also in 2016, the Directive on security of network and information systems (*NIS Directive*) was adopted. Transposed into French law in 2018, this first EU legislation on cybersecurity established a framework for the development of European standards based on criteria common to operators of essential services (OES).

Taking a new step in the policy of European cooperation on cybersecurity, the European Parliament and the Council of the European Union (EU) adopted in 2019 (March and June, respectively), the **European regulation known as the *Cybersecurity Act***, which provided for the creation of a set of **certification systems at the EU level**, and an **EU Cybersecurity Agency**. This regulation established a framework for cybersecurity certification in order to harmonise at the EU level the evaluation methods and the various levels of assurance of certification. Also in 2019, the Council established a framework enabling the EU to impose targeted restrictive **measures aimed at discouraging and controlling** cyberattacks threatening the European Union or its Member States "*including cyberattacks against third States or international organisations where restricted measures are considered necessary to achieve the objectives of the Common Foreign and Security Policy (CFSP)*".

In the US

In the 2005 *Energy Policy Act*, US authorities included major cybersecurity development focuses applied to the energy sector and electricity in particular. Under the Act, a private organisation, the *North American Electric Reliability Corporation* (NERC), was designated an *Electric Reliability Organization* (ERO) in order to establish security standards for the electrical grid at the Federal level, under the authority of the *Federal Energy Regulatory Commission* (FERC).

A series of standards aimed at electricity production and transmission infrastructures thus came into being in 2008: NERC-CIPS (*Critical Infrastructure Protection Standards*). Among the

most detailed standards in the world they are mandatory for the 3,000 electrical *utilities* in the United States.

2. Standards

Alongside national and international regulations, there are a number of standards governing the electricity sector. A brief, overview of the principal standards:

- **IEC 62443:** international standard establishing a cyberdefense framework for industrial systems. Previously, IT system security had been governed by ISO 27000, and, in parallel, industrial security fell under IEC 61508 and specific industry standards. IEC 62443 now combines both environments.
- **IEC 62645:** a set of measures for preventing, detecting, and responding to malicious acts committed by cyberattacks on the IT systems of nuclear power plants. It is aligned with the changes in ISO/IEC 27001 and takes into account technical developments and different national cyber protection practices.
- **IEC 62859:** a framework for managing interactions between security and cybersecurity for nuclear power plant systems. It adapts and supplements ISO/IEC 27001 and ISO/IEC 27002 within the nuclear context and is coordinated with the IEC 62443 series of standards on cybersecurity in industrial automation and control processes.
- **NERC-CIP:** North American standards applicable in all installations in the US and Canada producing or transporting electricity above a threshold of 1,500 MW. They cover all security aspects, including the process for reporting an incident, and the disaster recovery plan (DRP).
- **IEC 61850:** communications standard used by substation protection systems in the electrical energy sector. This standard is specifically used in exchanges between smart electronic devices (even those from different manufacturers) located at the level of the distribution stations of a power grid.

3. Electrical infrastructure protection in practice

Various solutions may be used to ensure the security of an energy infrastructure's sensitive equipment. Several of them should be included in an in-depth defence strategy, confronting cyberattackers with independent layers of protection of different types, which take up the slack in the event one of them fails.

Thus a good level of security can be achieved by respecting basic security principles, like separating IT and OT networks, segmenting the OT network, using firewalls, changing the default authentication elements of system equipment, and requiring employees to use digital hygiene measures (such as enabling logins on controlled terminals only, or preventing physical or digital storage of unencrypted passwords).

Stormshield solutions

But in order to implement such security systems, electrical infrastructures, due to their specificities, require appropriate means of protection. For years, Stormshield has been developing innovative solutions to do this, working in co-production with the biggest names in the sector, including Schneider Electric and Siemens, as well as French rising stars like Seclab.

Among its range of products, Stormshield has developed solutions in order secure operational messages, particularly with the control of protocols specified by IEC 61850 for power distribution grids. "*By analysing and filtering data passing through the instructions and protocols exchanged on our systems, our solutions help to reduce the risk of illegitimate orders*", says Tarik Zeroual, Global Account Manager for Stormshield. What's more, the SNi20 industrial firewall stands up against electrical environmental constraints with an IEC 61850 certification.



SNi40

SNi20

Stormshield

Industrial Security

V. And what will there be tomorrow?

The world of electrical energy is still the preferred playground of cybercriminals... Particularly because they also serve as a virtual territory in which certain states wage a battle, often unknown to the general public.

1. Toward accelerating geopolitical tensions

Once a cyberattack is detected against an electrical infrastructure, whether it causes significant damage or not, the question of the perpetrator arises immediately. What country is behind it? What were its true intentions? How to reassure the citizens, as the case may be? How to respond if the attack is actually part of an ongoing conflict with another nation?

For the past several years, cyberspace has become a zone for tests and demonstrations of force, before being that of open conflicts. The examples presented in this white paper are many, between Russia, which is no stranger to the two blackouts suffered by Ukraine in 2015 and 2016, and the US power grids which were regularly infiltrated in 2017, also by the Russians, and which were coveted by Iranian cyber-criminals since 2019. Not to mention the flurry of activities conducted by North Korean and Chinese cyberspies, and western powers, which are also not to be forgotten.

Faced with this unsettled, noxious digital environment, which some are calling a cyberwar, how should states respond? According to Julien Nocetti, researcher with the Institut français des relations internationales, "*the current trend is to reinforce the cyberdefense capacities of states. All cyberdoctrines developed by the West in recent years stress capacity, human, and financial reinforcement of defensive and offensive cyber warfare*".

2. Is Europe ready to deal with this?

A few years ago, the answer was not reassuring. European electrical grids were already heavily interconnected but, in parallel, Europe suffered from a lack of harmonisation of the cybersecurity strategies of its Member States. Certain countries (Greece, Denmark, Sweden, etc.), still had not developed a national cyberdefense policy or a protection plan for their critical infrastructures (Portugal, Luxembourg, etc.). It was as many breaches in the European electrical grids that proved worrying. Indeed, it was imaginable that an attack targeted against a less-protected system could spread beyond the borders of the country concerned, like the (non-cyber) incident between Italy and Switzerland in 2003, which spread to Slovenia.

European authorities, however, fully grasped the importance of encouraging Member States to get up to speed, and 2018, in particular, was marked by the national transpositions of two directives: NIS and SRI. Where the NIS directive required the identification of OESs, the SRI directive required the establishment of a national cybersecurity strategy. The SRI directive also

required each Member State to create a national call centre (CERT) and to organise procedures for the notification of national authorities by critical operators in the event of an incident. In parallel, the European Commission had established, starting in 2014, a funding plan (*Connecting Europe Facility*) totalling 60 million euros over seven years (2014-2020) in order to help the less advanced states to acquire equipment and training. A partnership with the *European Cyber Security Organization* also came into being in 2016 in order to stimulate cyberdefense research.

All of those efforts resulted in a rather reassuring result: in 2020, all of the countries in the European Union have at least a national cybersecurity policy, and most have established a protection plan for critical infrastructures, according to the *National Cyber Security Strategies - Interactive Map*, viewable on the ENISA website. Even if zero risk does not exist, this harmonisation of European responses to cyberthreats helps to severely reduce exposure of electrical systems to risks and to improve their resilience in the event of an incident.

Nearly

80%

of French companies have acknowledged having difficulties in recruiting cyber-specialists

3. Are companies in working order?

Confronting the speed and technical complexity of cyberattacks requires responsiveness. Companies therefore must be able to count on staff who are trained and led. That is one of the principal issues of tomorrow. Nearly 80% of French companies have acknowledged having difficulties in recruiting cyberspecialists, according to a study conducted by the Vanson Bourne. Training teams and spotting talents must therefore be one of their priorities now.

The awareness of the existence of cyber-risks by all actors in the electrical world also represents a sizeable challenge, which may seem paradoxical. Indeed, how can one imagine specialists in the electrical sector not being aware of such questions and organised to face them? Yet, for example, we still see connected equipment sold without any level of security. Service providers, and more broadly the whole supply chain for electrical companies, also represent potential risk vectors. And, more indirectly, any other economic actor participating at its level in the ultra-connection of IT systems as well. In order to best respond to this threat, companies in the sector appear to be reinforcing cybersecurity management through dedicated budgets, work on crisis plans, or raising awareness and training of teams.

Lastly, and luckily, while cybercriminals don't hesitate to communicate with one another, and even exchange practices, private companies are

not inactive and isolated. Many have understood that it is important to know what threats they face and how they arise. Companies are also increasingly daring to communicate about the attacks they have suffered in order to help private and public sector organisations to best detect and anticipate coming risks. Thanks to this approach of cooperation and sharing knowledge on cyber threats, to be conducted relentlessly, future attacks may be absorbed more easily.



Bibliographic references

Observatoire de l'Industrie Électrique, *La cyber résilience des système électriques*, November 2017, https://observatoire-electricite.fr/IMG/pdf/oie_-_note_conjoncture_-_cyber_resilience_des_systemes_electriques_-_novembre_2017.pdf

Long form in Numerama, *Ukraine, anatomie d'une cyberguerre — épisode 1 : la menace au quotidien*, 5 September 2017, https://www.numerama.com/politique/283573-en-ukraine-la-cyberguerre-au-quotidien-episode-1-la-menace-permanente.html

Article in Futura Sciences, *Le malware Crash Override-Industroyer est-il plus redoutable que Stuxnet ?*, 13 May 2017, https://www.futura-sciences.com/tech/actualites/informatique-malware-crash-override-industroyer-il-plus-redoutable-stuxnet-25307

Press release from Le Point international, *États-Unis : un fournisseur d'électricité piraté par des Russes, 31 décembre 2016*, https://www.lepoint.fr/monde/etats-unis-un-fournisseur-d-electricite-pirate-par-des-russes-31-12-2016-2093899_24.php

Article in L'Usine Digitale, *Elexon, maillon crucial du réseau électrique au Royaume-Uni, victime d'une cyberattaque*, 15 May 2020, https://www.usine-digitale.fr/article/elexon-maillon-crucial-du-reseau-electrique-au-royaume-uni-victime-d-une-cyberattaque.N964926

Article in L'energeek, *Le coordinateur européen des transporteurs d'électricité victime d'une cyber-attaque*, 11 March 2020, https://lenergeek.com/2020/03/11/coordinateur-europeen-transport-electricite-cyber-attaque/rique-au-royaume-uni-victime-d-une-cyberattaque.N964926

Column in Libération, *L'attribution des cyberattaques, un bras de fer diplomatique*, 5 October 2018, https://www.liberation.fr/planete/2018/10/05/l-attribution-des-cyberattaques-un-bras-de-fer-diplomatique_1683201

Column in Libération, *Les cyberattaques sont des fantômes*, 17 March 2019, https://www.liberation.fr/planete/2019/03/17/les-cyberattaques-sont-des-fantomes_1715230

Report from the *Office of Technology Assessment, What happens during a blackout: Consequences of a prolonged and wide-ranging power outage*, 2011, https://www.tab-beim-bundestag.de/en/pdf/publications/books/petermann-etal-2011-141.pdf

Report by Lloyd's and the *Centre for Risk Studies of the University of Cambridge, Business Blackout*, 6 July 2015, https://www.lloyds.com/news-and-risk-insight/risk-reports/library/society-and-security/business-blackout

Article in 01.net, *Compteur électrique intelligent : quand le hacking mène au black-out général*, 17 October 2014, https://www.01net.com/actualites/compteur-electrique-intelligent-quand-le-hacking-mene-au-black-out-general-628914.html

Publication by the Institut français des relations internationales, *Cyberattaques et systèmes énergétiques : faire face aux risques*, 2017, https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cybersecurite_2017_2.pdf

Publication by the Institut français des relations internationales, *Cybersécurité des infrastructures énergétiques : regards croisés Europe/États-Unis*, 2018, https://www.ifri.org/fr/publications/etudes-de-lifri/cybersecurite-infrastructures-energetiques-regards-croises-europeetats

Forum by Nicolas Mazzuchi on L'energeek, *Cybersécurité et énergie : une complémentarité fondamentale*, 21 October 2019, https://lenergeek.com/2019/10/21/cybersecurite-energie-renouvelables-attaques-nicolas-mazzuchi/

Report by Thales & Verint, *Cyber Threat Handbook Thales – Verint*, 10 July 2019, https://www.thalesgroup.com/en/group/journalist/press-release/cyberthreat-handbook-thales-and-verint-release-their-whos-who

Report by Thales - General Electric, *Report on Cyber Threats to Operational Technologies in the Energy Sector*, 2020

Decree No. 2006-212 of 23 February 2006, and French Act No. 2013-1168 of 18 December 2013, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028338825/2020-0928/

Press release from the Council of the European Union, *Cyber-attacks: the Council is now able to impose sanctions, 17 May 2019*, https://www.consilium.europa.eu/fr/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

Article by Usbek & Rica, *Nous sommes dans une situation de cyberguerre froide*, 30 April 2019, https://usbeketrica.com/fr/article/nous-sommes-dans-une-situation-de-cyberguerre-froide

Web page of the Commission de régulation de l'énergie, *Électricité : Interconnexions*, 17 December 2019, https://www.cre.fr/Electricite/Reseaux-d-electricite/interconnexions

Interactive map by ENISA, *National Cyber Security Strategies - Interactive Map*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

STORMSHIELD

The European cybersecurity choice

All over the world, companies, government institutions and defence organisations need to be able to rely on trusted partners to support their digital transformation and provide cybersecurity for their infrastructure, users and data. Stormshield technologies are certified at the highest European level (EU Restricted, NATO Restricted, Common Criteria EAL3+ / EAL4+, ANSSI qualifications and visas), and address IT and OT challenges to protect your business activity. **Our security solutions restore your freedom to do business with complete peace of mind.**

www.stormshield.com

All distribution, reproduction or representation, even in part, of this white paper, for purposes other than private use, regardless of medium, is prohibited, and could engage the civil and criminal liability of any person who fails to comply with this prohibition.