# Power networks as targets: hazards, vulnerabilities and protection of electricity networks from the Second World War to 21st century asymmetric conflicts

Angélique Palle

# Power networks as targets.
# Hazards, vulnerabilities and protection of power networks, from the Second World War to the 21st century asymmetric conflicts

*Angélique Palle*

Palle, Angélique. « Power networks as targets: hazards, vulnerabilities and protection of electricity networks from the Second World War to 21st century asymmetric conflicts ». *Flux* 118, nº 4 (2019): 46-58. https://doi.org/10.3917/flux1.118.0046.

## Introduction

Electricity transmission networks are historically part of strategic infrastructures protected by national defense. Targeted as war objectives for destruction during the Second World War (Bongrain 1994; Barrère, 2002), they received special attention from the Allies during the reconstruction and the Cold War (Lagendjik, 2008). If the peace and the construction of Europe have diminished the risk of physical destruction in wars, the rise of asymmetric conflicts and terrorism have led since the 2000s to new physical and cybernetic hazards for these networks. The United States (US), the European Union (EU) and France have then defined and identified (partly in response to the attacks of 11 September 2001) several "critical" infrastructures, including electricity networks. The recent 2019 blackouts affecting Venezuela have shown how vital for society and state stability power networks are today.

The evolution of their role in western capitalistic societies and their increasing influence as the electrification of energy uses grows[1], whereas the power sector is at the same time undergoing deep changes through energy transition, climate change mitigation or sustainable development dynamics, calls for a renewed analysis of their exposure to risk. Risk is understood, in this paper, as a function of hazard and vulnerability, mitigated by a potential resilience (Reghezza, Veyret, 2003, 2006).

This paper thus aims to analyze these new hazards and the vulnerabilities that recent changes in this networks' environment have brought. It then seeks to compare the reactions of the EU, of France and of the US to what are perceived as new threats. The point here is not to suggest technical resilience prospects[2], but to explore how the US and the EU have comparatively built a risk culture around these risks and how they manage them. The analysis relies on various field and technical collaborations in EU and in the US[3], whereas most of the technical data stem from incident reports, security guidelines, stress test feedbacks and risk assessment from the network operators.

We will first analyze the recent evolution of the status of these networks that serve as a base for the entire economy and lifestyles of Western societies. From war goals for destruction in the twentieth century, they have become in the last ten years targets for physical sabotage (with the example of the Metcalf substation powering the Silicon Valley in 2013) or cybernetic attacks (Ukrainians and Baltics cases). This analysis will then be

[1] Enerdata, 2019, Global Energy Statistical Yearbook 2018, (accessed 30 January 2020), Available at: https://yearbook.enerdata.net/

[2] The term of resilience is a complex issue regarding power networks. It is generally understood as an equivalent to a return to the previous normal operating conditions by the technical operators. Geography on the other hand gives a broader and more changing sense to the term (Reghezza-Zitt, Rufat, 2015).

[3] This paper is based on the results of a Ph.D carried out from 2012 to 2016 on the European electricity networks, including their vulnerability; continued by a comparison with US networks at a two-month research residency at the Electrical Engineering Department of Cornell University (USA) in 2016; as well as a collaboration on scenario building and stress tests conducted in 2018 with M2 students from the School for Computer Science and Advanced Techniques (EPITA), on the vulnerabilities of the French network.

confronted with the new vulnerabilities induced by the integration of networks on a European scale which favors waterfall effects (case of the European blackout of 2006) and by the energy transition that opens networks to digital controls and makes them more vulnerable to cyberattacks. Thirdly, a comparative analysis of the American, European and French responses to these new risks weighing on the networks is proposed. The analysis starts from the results of the GridEx exercises conducted in the United States, which bring together all the actors in the US every two years, around simulations of cyber and physical attacks combined.

## Power grids, from war objectives to critical infrastructure

For the last century, electricity networks have been targeted by different types of actors and attacks. Targeted for physical destruction by the armies during the first two World Wars, they are now the targets of more blurred types of actors that lead attacks of different natures which could rather be categorized as sabotage.

*From the second World War to the Cold War: destructions and sabotage, the strategic dimension of electricity transmission infrastructure*

The European states, particularly Germany, Belgium, France, the Netherlands and Italy, prepared for the Second World War by integrating their electricity networks, as well as the associated control and dispatch centers, at a national scale (Lagendijk, 2008). The aim was both to strengthen the network in the event of conflict and to enable it to support an economic war effort. The French national interconnection program, launched in June 1938, thus considered the construction of lines as an objective of national interest regarding both the economy and the defense of the country (Bongrain, 1994). One-third of the funds allocated to the planned development of this network were for projects (power lines) marked as "national defense". The main aim was to strengthen the network in north-eastern France and electrify the Maginot line (turrets, ventilation, electric traction supply trains, etc.) (Bongrain, 1994; Morsel, 1994). A special police force was formed to guard and protect the electrical infrastructure. The Germans did the same during the occupation and two regiments were assigned to protect the strategic line linking Paris and the Massif Central (Bongrain, 1994).

During the occupation of France by the German troops, the electrical system has been particularly subject to sabotage by the French resistance. If history and collective memory recalls more easily the sabotage of trains and communication lines, the government of Vichy records 277 actions led against the power system in the North region between November 1943 and April 1944, and two important underground missions, Josephine B. and Armada, targeted the power system (Albertelli, 2016). The first one is the first important success of the Special Operation Executive[4] in France, the second one in 1943 marks the beginning of a sabotage campaign led by the resistance in France to avoid massive bombing and destruction by the British of strategic infrastructures.

At the end of the war, restrictions, bombings and sabotage had virtually paralyzed the French high-voltage transmission system. As for production, it had fallen by 30% between 1939 and 1944. The allies then made restoring the country's electricity supply and network rehabilitation one of their priorities (Lagendijk, 2008). During the Cold War years, electricity supply infrastructure remained a strategic issue. The repair of the West Berlin Power Station, which had been damaged and partially dismantled by Soviet troops, was, for example, one of the stakes of the US airlift during the Soviet blockade of the city until May 1949 (Lagendijk, 2008).

During the 20$^{th}$ century, power networks have been subject to rather identified dangers. Targeted by armies and resistance movements during the second World War they are still identified by them as strategic infrastructures during the Cold War. They are subject to both destruction, which refers to the bringing down of material elements, and sabotage, which is a more specific complete or partial damage, embedded in a strategy, often carried out secretly and using a disproportion between the weakness of the means used and the wide extend of the results obtained (Albertelli, 2016). Both damages and protections are then carried out by military actors or according to military purposes and are part of a global war strategy.

*The 21$^{st}$ century: Asymmetry of conflicts and the emergence of "critical infrastructure"*

With peace and the construction of Europe, the electricity transmission infrastructure, while maintaining its economic importance, has seen its strategic importance diminish for the armies as it was no longer threatened by conventional conflicts. The growth of asymmetric conflicts and the rise of terrorism since the beginning of the

[4] A British intelligence service operating during the war with the mission to help local European resistance movements.

2000s have once again made these infrastructures, essential to industrialized capitalist economies and societies, potential targets.

From the 1990s, the growing number of asymmetric conflicts and the modes of action, particularly terrorist ones, which characterize them have reinforced and changed the nature of potential threats weighing on these networks. Following the attacks of 11 September 2001, the United States, the EU and its Member States have gradually redesigned their approach for the protection of the "critical infrastructures" of which these networks are part. The cyber-attacks against the Ukrainian network in the winter of 2015, in a context of conflict with Russia, have also revived the interest of the states in these infrastructures (see the following part on vulnerabilities).

The supply of electricity is essential for the maintenance of a large number of vital functions in capitalistic and globalized societies. One example among many, in 2003, a blackout in the United States critically increased the risk of an outbreak in Detroit by preventing the cleansing of conduct of the water supply network. The notion of "critical infrastructure" thus appeared in US official texts in the mid-1990s. In 2001, the attacks of September 11 and the Californian energy crisis led the White House to define a national strategy for their protection. It has been reflected by the transformation in 2003 of the Office of Internal Security into a ministry, with one directorate particularly in charge of the infrastructure issue. The concept spread in Europe in the mid-2000s[5], especially after the attacks in London and Madrid.

Definitions and approaches to these critical infrastructures vary. Some like Canada or Germany have adopted an initial multi-hazard approach. Others like the United Kingdom or the United States have focused their protection policy on the terrorist threat. France has adopted an intermediate position and instructs its ministers or prefects to designate in their area of responsibility the "vitally important operators" tasked with identifying "points of vital importance" and putting in place "safety plans" (Galland, 2010). It concerns infrastructure "whose unavailability could significantly reduce the potential war or economic, security or the ability of the nation to survive"[6]. The manager of the French electricity transmission network, RTE, has thus been designated as an operator of vital importance (OIV) in 2008, within the framework of the National Energy Security Directive, and counted in 2012 about 50 points of vital importance (PIV)[7].

## Specific vulnerabilities vs. new vulnerabilities

Power networks have thus been labelled as critical or vital infrastructures. They are subject to both specific and new vulnerabilities which we analyse in this second part, both from a conceptual and a practical aspect before combining this analysis with the study of the threats that affect them.

*The concept of risk applied to power networks*

Analysing critical infrastructures such as power systems falls within the conceptual domain of risk, which we use in this paper as it is used and defined by geographers and planners working in particular on natural, industrial or societal risks (Reghezza, Veyret, 2003, 2006). The risk is, in this field, function of three components:

- The hazard, which is the probability of occurrence of an event (flood, technical incident, etc.).
- The vulnerability, which is the propensity for a material or human stake to be affected by this hazard (presence of dike or specific architectures designed to withstand the hazard).

[5] European Commission, 2006, Green Paper on a European Critical Infrastructure Protection Program (EPCIP) ; Council Directive 2008/114 / EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection ; Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a common high level of security of networks and information systems in the Union.

[6] French Defense Code - Articles L. 1332-1 to L. 1332-7, L. 2151-1 to L. 2151-5 and R. 1332-1 to R. 1332-42 ; Interministerial Instruction No. 6600 on the safety of life-saving activities of 7 January 2014 ; Law No. 2013-1168 of December 18, 2013 relating to the military programming for the years 2014 to 2019 and bearing various provisions concerning the defense and the national security, art. 22 ; Law No. 2018-607 of 13 July 2018 relating to military programming for the years 2019 to 2025 and bearing various provisions concerning the defense, art. 18 to 22.

[7] Max Ernoult, Assistant Secretary General for Defense and Security, RTE, 2012, Cycle of IHEDN meetings, Paris-La Défense, 23 October 2012.

– The resilience, which is its ability to regenerate in a given time to eventually reach a return to the initial situation. In this paper we focus on hazard and vulnerability. Resilience, although it is present in the last part of the paper, is not subject to a specific treatment.

In the case of a power network, the hazards we are interested in are either physical or cyber. The vulnerability of the network depends on the accessibility of the infrastructures, their state, their redundancy (is there only one or more supply roads for a territory?) (Baran, 1964). Resilience is determined by the ability of the network manager (the transmission system operator, TSO, in this case) to respond quickly, to have replacement hardware, to communicate with other managers of neighbouring networks –in case of network interconnection– as well as with the police or military according to the case.

The very structure of networks induces certain types of vulnerabilities (Gleyze, 2005). A power network can be modelled as a combination of nodes and links with the particularity that the power frequency on the network must be the same at all times (the system is called synchronous). This means that the destruction of a small number of either nodes (substations, injection or withdrawal points) or links (power lines) has a huge effect on the entire system (Kempf, 2014). To cope with this structural vulnerability, transmission system operators have (within the EU) defined a set of rules to ensure a minimum of robustness in their networks. The main one, the *n-1* rule, states a TSO should ensure that the network should continue to work despite the loss of any single element of the network (either link or node). The functioning of the network despite the loss of a combination of elements deemed probable is also ensured[8].

In this broad context, the SESAME research programme (Securing the European Electricity Supply Against Malicious and accidental thrEats)[9], financed by the European Commission within the 7th Framework package European Union research and development funding programme and led by the Politecnico di Torino, defined the following types of risk for power networks:

| **Risk assessment for the French power network (SESAME programme)** | | | | |
|---|---|---|---|---|
| *Risk* | *Aspects* | *Weak (1-3)* | *Mild (4-7)* | *High (8-10)* |
| Economic | Inadequate investment, changing demand | | | 8 |
| Technical | Distributed generation, new technologies | 3 | | |
| Topography | Weather, natural disasters | 3 | | |
| Social | Terrorism, political instability, demonstrations | | 5 | |

*Source : SESAME/Heriot-Watt University, Assessment of Security of Electricity Supply (SES) Indicators in Europe, Délivrable n°D3.1, 2014.*

*New vulnerabilities, digitization, energy transition, integration*

If power systems present overall structural vulnerabilities, they are also affected by the conjunctural evolution of their environment. In this respect, two ongoing trends have opened new vulnerabilities in the power systems of capitalistic globalized societies.

The first one relates to the dynamics of the energy transition. In order to increase energy efficiency[10] and technical optimization, networks have opened up to digital technology. The evolution of their control systems

[8] RTE, 2006, Technical Reference Manual, Chapter 7. Management and operation of the network, Article 7.1 Security of the system - Associated rules.

[9] Website of the SESAME project: www.sesame-project.eu

[10] Energy efficiency, used in the broad sense of the term, refers to all technologies and practices that reduce energy consumption while maintaining the same final service (definition proposed by the French Energy Regulatory Commission, CRE).

and the inclusion of certain computer components allow real-time information on the state of the network to be traced back to the control centers. This have also made them vulnerable to cyberthreats. The goal of this evolution is to send not only electricity but also real-time information within the network in both directions, which has led to call this technology and network structure "smart grid". This policy leads, for example, in a more or less conscious and voluntary way, to the connection of certain infrastructures to the Internet which makes them vulnerable to hacking[11]. In March 2007, researchers at the Idaho National Lab (USA) conducted the "Aurora" test in which they succeeded in manipulating the control systems of a diesel-powered electric generator using a computer virus. By adjusting the rotational speed of some of its parts, they stopped the operation of the generator. This test was at the time particularly conclusive because it demonstrated the possibility for a cyberattack to cause physical damage to the network infrastructure[12].

The second trend concerns more specifically the European Union and is related to the dynamics of European integration. The EU energy policy as defined by the Treaty of Lisbon promotes the integration of energy networks, both to enable the establishment of a large common market and to achieve economies of scale[13]. However, this interconnection also increases the waterfall effect and propagation in the event of an incident. The last major European blackout (2006) generated by an incident on a German line has thus affected 15 million consumers in 12 countries within the Union and close neighborhood (Palle, 2016). The effects of this interconnection of European networks today makes it impossible to adopt a purely national approach to their protection. The interconnected European network now brings together 42 network operators and they must interact to ensure security of supply for the European area. The structure and dynamics of American networks are different from those in Europe. If the EU has been integrating the electricity transmission networks of its member States since the end of the 1990s, the integration of the networks of the various States has never been an objective for the United States. The ownership and management of these networks is the result of a plurality of operators who play a lesser role than the European network operators. However, the North American regulator (NERC) is much more influential than the European regulatory agency (ACER, created in 2011). These structuring differences, as well as the condition of the network, which is generally more obsolete in the United States, play a role in the way the EU and the US approach the protection of their electricity network (see *infra*).

## From the evolution of threats to the change in risk culture

Combined to the structural and current conjunctural vulnerabilities of power systems, two types of specific threats have developed since the beginning of the 21st century, physical and cyber ones.

*Physical threats*

If physical hazards linked to technical failure of some components or to natural disasters have been known by system operators since the beginning of electricity systems, the malevolent degradation or destruction of elements of the network follow a different path. Power systems were subject to destruction and sabotage during the Second World War and the cold War (see *supra*) as part of a wider plan within a conventional conflict. The trends since the beginning of the 21st century have been different and physical attacks against the power system are now considered within a wider response to terrorism or in asymmetrical conflicts. The 2013 attack on the Metcalf substation powering the Silicon Valley in California has been the starting point for the realization, in the United States, of a specific physical vulnerability of power grids that the general infrastructure protection framework of the country did not then allow to take into account effectively.

On April 16, 2013, around 1 am, the Californian sub-station Metcalf, located southeast of San Jose and managing the power supply of the Silicon Valley, was attacked with AK-47. After cutting off the telephone and Internet wires, the attacker(s) put off, in less than 20 minutes, 17 transformers from the substation. As it was not

---

[11] Mc Afee, *Smarter protection for the smart grid*, 2012, [Online] (accessed 30 January 2020) Available at: https://www.ccn-cert.cni.es/.../rp-smarter-protection-smart-grid.pdf.

[12] Aurora test, CNN Video [Online] (accessed 30 January 2020). Available at: https://www.youtube.com/watch?v=fJyWngDco3g ; Center for the Study of the Presidency and Congress, Securing the U.S. Electrical Grid, The Honorable Thomas f. Mclarty III & the Honorable Thomas J. Ridge, 2014, [Online] (accessed 30 January 2020) Available at: https://www.thepresidency.org/sites/default/files/Final%20Grid%20Report_0.pdf

[13] The interconnection of Germany, France and Benelux reduces the production capacity required for their supply by 2%. RTE, 2015, Ten-Year Network Development Plan, 2014 Edition, p.15.

particularly strategic for the network, the blackout was avoided, but it took 27 days and $ 15 million to repair the equipment[14]. Transformers have the function of increasing or decreasing the voltage of the lines, thus making it possible to reach the high voltages required for the transmission of electricity over long distances. Long to manufacture (sometimes more than two years), they can cost several million euros and are difficult to transport. During the attack on the Metcalf substation, the shooters mainly damaged the cooling structures. The operation of the substation was stopped before a serious overheating of the equipment, which made it possible to avoid more heavy damage.

Like Metcalf, substations are mostly located in sparsely populated areas and are poorly protected, often by simple metal chains and cameras. This is to prevent theft of equipment which is the main risk for these infrastructures today. In this case, the cameras did not identify the shooters, located outside the surveillance perimeter. A year after the attack, the same substation was the subject of a theft of equipment (August 2014), without the alarm systems reacting. This incident led to a wider reaction both from the utilities and the federal government regarding the protection of power networks. However, the SESAME research program conducted in the EU concludes that if the main hazards that statistically affect power networks are due to technical failures and human errors, it is on the other hand very difficult to estimate the impacts of "non-standard" hazards (Hoffmann, Caramanis 2019), such as terrorist attacks, on infrastructures which safety margins have been reduced in recent decades and which operate more and more frequently in situations of tension[15].

*Cyber threats*

If the nature of physical malevolent damages and threats to the power systems has changed with the 21st century and now concerns less identified actors operating within different framework (outside of a military strategy or in a similar case), cyberthreats are a new trend in comparison.

In Europe, the first cyber-attack against a European network operator and officially confirmed by him (50Hertz, German network operator) took place in 2012[16]. Though not serious for network stability and security of supply, it nevertheless lasted five days before a solution for a return to normal condition of operation was found. Five years later, in 2017, 80% of EU companies reportedly experienced at least one cyber incident and 400 billion dollars were lost because of cyber attacks in the EU in the last few years[17]. If these attacks mainly target private or public firms for ransom, they also take place in conflictual context between two states or a state and non-governmental actors.

On December 23, 2015, a blackout in Ukraine attributed to a cyberattack perpetrated against the electricity transmission network affected about 225,000 consumers. The attack targeted the network infrastructure control systems but also directly seven substations whose network operators could not regain control of and which required the dispatch of maintenance teams to carry out inspections and repairs on the affected substations. Operator phone lines had also been scrambled. The attack was attributed by Ukraine to Russia, with which it has been in open conflict for more than a year. This is the first cyberattack officially recognized as "successful" by a State against its power grid[18]. The US have more recently claimed to have both breached into the Russian power grid and been the target of similar successful intrusions[19].

---

[14] Harris S., 2013, "Military-Style" Raid on U.S. California Power Station Spooks, *Foreign Policy*, December 27; Rosato J. Jr., 2014, Following Attack on PG & E Substation, Bill Requires California Utilities to Beef Up Security, NBC Bay Area, March 10.

[15] SESAME (Delft University of Technology, Politecnico di Torino, INDRA et Transelectrica), 2012, *System Specification of Decision Support System*, Délivrable n°4.1.

[16] Nelsen A., 2012, European renewable power grid rocked by cyber-attack, *Euractiv.com*, December 10.

[17] Dominique Ristori, Director General European Commission / DG ENER, conference held by the Austrian presidency of the European Union, October 11, 2018, Brussels.

[18] US Department of Homeland Security, Cyber Emergency Response Team, Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure, February 25, 2016. [Online] (accessed 30 January 2020) Available at: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[19] Sangers D. E., Pelroth N., 2019, U.S. Escalates Online Attacks on Russia's Power Gid, *The New York Times*, June 15, 2019.

Protective and mitigation measures against cyberthreats are still being investigated. They include putting off the grid some specific strategic infrastructure (which already have emergency supply structures in many cases). The US Army has thus been testing off grid systems for some military bases (Fort Bliss, Texas), also partially to reduce the cost of the army's consumption as they are based on renewable consumption. Some European power system operators[20] also suggest shifting from a security by default to a security by design paradigm. This implies abandoning the idea of entirely protecting the entire network and choosing which parts should be focused on. Keeping active the old manual control systems (which helped mitigating the effects of the attack in Ukraine). As a general rule though, State, defense and network actors agree on the idea that for now, soundly protecting power grids from cyberattacks from a technical perspective is difficult because the old control systems have been built without today's security issues in mind and cannot be updated, some parts of the network are increasingly connected to the internet, and the new generation of smart grids and connected devices enhances this tendency as they often lack strong security standards.

*Awareness and risk culture*

Confronted with the new aspects and combination of threats and vulnerabilities that affect the power systems, the actors of the energy domain progressively took specific measures to protect them.

In the US, the attack of the Metcalf substation revealed that the protection of the American power grid had been left in the hands of the sole transmission system operators who manage the networks and that no federal agency was responsible for it. The reaction of the American regulator and the covering of the attack by media led to a reframing of the protection system and of the associated stress tests that were conducted on the networks since 2011[21] (see following part).

In the EU, the risk culture for these combinations of threats and vulnerabilities is recent. According to the interviews conducted with them in 2014[22], the electricity system operators in charge of their maintenance, stability and development perceived these networks mainly as service infrastructures. As such, they felt relatively disconnected from the strategic aspects regarding defense or State security. The challenges of harmonization of European rules and cooperation, to enable the establishment of the large common energy market desired by the European Union, as well as the need to adapt the networks to the changes brought about by the dynamics of the energy transition, have until very recently absorbed all the vital forces of a sector in profound change. The Directive on security of network and information systems (the NIS Directive) that was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016 after four years of negotiations, along with the rise of attacks and of their mediatisation, shows a change of the culture. Member States had to transpose the Directive into their national laws by 9 May 2018 and identify operators of essential services by 9 November 2018. In this context the speeches and exchanges held at the Conference on cybersecurity in the energy sector, co-organised by the European Commission, the Austrian Federal Chancellery and the German Economic Institute on the occasion of Austria's EU Council Presidency on 11 October 2018 show on the contrary strong interest among the European energy actors and the awareness that an interconnected network implies cooperation.

Research trends follow the same pattern in the EU which supports a number of research projects on these issues. As part of the EU's 7th Framework Program for Research and Technological Development, the SESAME project (Securing the European Electricity System against Accidental and Malicious Threats), co-financed by the European Commission, is thus the translation of an awareness of these new risks. Coordinated by the Politecnico di Torino, the research consortium brings together Italian, Austrian, Spanish, Dutch, Romanian, EU and UK research and industry stakeholders.

This program has been based on the following observation:

---

[20] "Cybersecurity in the energy sector", conference held by the Austrian presidency of the European Union, October 11, 2018, Brussels.

[21] Martinez M., 2014, Sniper attack on Silicon Valley grid spurs security crusade by ex-regulator, *Cable News Network*, 08/02/2014

[22] Interviews conducted within the European Network of European Transmission System Operators (ENTSO-E) in Brussels from January to July 2014.

> "The threats for the supply of electricity have changed dramatically throughout the last decade; additional to the natural (lightning, flood,…) and accidental ones (component failure, untimely intervention of protections,...), a new threat represented by highly organised malicious attacks needs to be considered in the light of the development of national and international terrorism and crime. All energy grids are exposed to threats of different kinds, like physical attacks to key assets (e.g. substations), cyberattacks to their control systems, and use of electromagnetic bombs to deafen key control stations. Such attacks might be jointly imparted so as to affect large portions of the European grid, make repair difficult and cause huge societal impact. Pressure to ensure security of critical interconnected infrastructures is very strong in the US, where there is a pungent push from the US government and an influential awareness by the main stakeholders. Until now EU industry awareness and readiness lagged behind, although the feeling that the issue is becoming crucial is now growing. It is believed that exposure to malicious threats is massively growing, to the point that intelligence sources estimate today a disruptive attack is more likely to target Europe than the US."[23]

The SESAME program was completed in the autumn of 2014. It was possible to follow some of the developments and conclusions, and to take part in its closing conference on 16 September 2014 in Brussels. Together with interviews conducted in the Security of Supply division of the Institute for Energy and Transport of the Joint Research Center of the EU (JRC-IET) in 2013[24] they lead to the following analyzes. The interest of the EU for research in this area has been confirmed during H2020 calls for projects and a call was issued for 2018 on network cybersecurity[25].

The security of the European network and electricity system is not strictly technical, and several decisions need to be made at the political level. The first is to define what is meant by security or safety of the network. They are functions of the level of investment that society is willing to consent to, to protect interests that regard economic, social and defense aspects. Absolute protection does not exist and a level of protection that is too high in relation to the probability of occurrence of an event, or the extent of its consequences, would constitute a significant economic and social cost. The definition of the acceptable level of vulnerability and the resilience (that is, the time and cost of a return to normal) expected from the network in the event of an incident cannot be left to the discretion of the managers alone. This requires both awareness and accountability of the political powers, as well as consumer awareness.

The operation of our electricity markets is also becoming increasingly centralized at the European level, but if this centralization process fails for some reason, we are now too interconnected for a possibility of return to national option in a short period of time. This *de facto* interdependence thus raises the question of the coordination and exchange of information at the European level for the safety of the network, even though this interconnection does not concern only EU member countries. Switzerland, Norway, Serbia, Bosnia and Herzegovina, Kosovo, Montenegro and Macedonia are interconnected with the various European synchronous networks and therefore cannot be left outside of technical and security cooperation without weakening the whole system.,

If the socio-economic impacts are significant and are estimated in terms of loss of GDP points, the question of the impact of a blackout in areas of defense and national security also arises. Infrastructures and strategic communication systems are generally provided with emergency electrical devices. It is necessary to ensure maintenance and coordination, which is sometimes neglected[26]. The 2003 blackout in the northeastern United States, for example, had affected some prisons and led to the revolt of several hundred prisoners (without, however, causing a major security breach). Government communication is also singled out in a number of these events: the message sent to citizens is sometimes poorly controlled, unclear or minimalist, which leads to

---

[23] SESAME website : https://www.sesame-project.eu/project/concept-and-objectives

[24] Interviews conducted at the JRC-IET on 21/05/2013 in Petten (Netherlands).

[25] Horizon 2020, Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches, Pillar: Societal Challenges, H2020-2018-2020, Secure societies - Protecting freedom and security of Europe and its citizens, Call : H2020-SU-DS-2018-2019-2020.

[26] SESAME (Transelectrica, Politecnico di Torino), 2011, *Report on the analysis of historic outages,* Délivrable n° D1.1.

tensions, or even panic reactions within populations[27]. The 2019 series of blackouts in Venezuela have recently opened a new perspective on possible state or society collapse induced by the failure of power networks.

## Institutional and practical structuring of risk management, the American and the European approaches

In the light of the evolving awareness of both power grid vulnerability and threats, this fourth part compares the institutional and practical structuring of risk management (hazard, vulnerability, resilience) on the European and American electricity transmission networks. Though both networks face partly similar risks, there is a difference between European and American protection strategies. Where the EU institutionally separates the management of these two types of threat, the American system manages this dual component in an integrated manner.

*The United States building a direct link between the federal government and the bodies responsible for protecting the network*

The US Department of Energy (DOE) began to focus on government-industry cooperation in protecting critical energy infrastructure in the late 1990s. It entrusted this responsibility to the North American Electricity Reliability Corporation (NERC), which is the international regulatory authority for the North American power transmission system. The involvement of the Department of Homeland Security (DHS) on the subject after the attacks of 11 September 2001 led to the drafting by the latter of a national plan for the protection of infrastructures in 2006. It created the Electricity Subsector Coordinating Council (ESCC), which takes over this coordinating role. As of 2013 and following the attack on the Metcalf substation (see *supra*), the CCHS also established a direct link between the federal government and the industry players for the protection of the network. The lack of real coordination at the federal level for the protection of the network as well as the lack of a national coordination plan had indeed been pointed out by the director of the Federal Agency for Energy Regulation[28]. No federal agency was officially in charge of the security of these infrastructures, this legislative void making the whole network security rely on the sole initiatives of the energy industry.

The industrial players involved in the operation of the electricity transmission networks also launched in 2014 a joint program for securing the network[29]. Running for two years, he had two goals. The first was to identify substations or combinations of strategic substations, that is, those whose decommissioning would be critical to grid stability, especially those interconnecting several high voltage lines with different voltages. The second was to establish possible strategies for reinforcing the resilience of the network: e.g. use of generation closer to consumption basins (though it implies higher costs) or separation of the network into several independent electric islands in case of destabilization, to reduce domino effects.

Since the early 2010s, the US power sector has rethought and restructured the protection of its networks considering the new cyber and physical threats identified. While the terrorist nature of the Metcalf substation attack in California has not been resolved, the event led the Department of Homeland Security to request the update of the National Report of the Research Council, "Terrorism and Electricity Distribution System", drafted in 2007 at its request and declassified in 2012. This report focuses on the vulnerability of the network as well as on ways to increase its protection and resilience along some major features:

- in a sector that is particularly complex on a technical level and where many actors interact, the emphasis is placed on information sharing and communication between actors of different natures (political, technical, defense and security) and acting at different scales (state or federal);
- a direct link between the federal government and industry has been established;
- attack simulation exercises involving all actors take place every two years to test network resilience and crisis management structures.

These features show the practical approach which is taken by the North Americans. The reactivity of the actors and the resilience of the network in the event of an attack are tested by stress tests called GridEx (for Grid

[27] Ibid.

[28] Martinez M., 2014, Sniper attack on Silicon Valley grid spurs security crusade by ex-regulator, *Cable News Network*, 08 February 2014

[29] Onishi N., Wald M., 2014, Months Later, Sniper Attack at Power Hub Still a Mystery, *New York Times*, 05 February 2014.

Exercise) which take place every two years since 2011. They aim at integrating these reflections. While the first GridEx was conducted on a regional scale[30], the following were of a much larger scale and they combine both cyber and physical attacks. GridEx II[31] was conducted in 2013 on a continental scale (Canada and Mexico also participated). Over 48 hours, the development of the simulation virtually plunged ten million Americans into the dark and caused the fictitious death of a hundred members of the police, or of the personnel of the companies involved in the exercise. The results of these first two exercises show, according to the reports, a good horizontal coordination of industry at the local or regional level, which deteriorates when it comes to communicating vertically, with regulators or federal agencies to manage crisis.

According to the reports, this lack of communication is due to internal protocol issues, a lack of a culture for cooperation with federal actors among industry players and a lack of confidence in them. As a result, the two following GridEx[32] (2015 and 2017) largely focused on improving communication and coordination between the various actors involved (the 2017 exercise involved around 5,000 people). Specific communication channels, a system for sharing information on the state of the network as well as a coordination of messages sent to the population have been put in place and tested.

*The European Union: an attempt at common governance*

The EU has been closely following the US initiative for the protection of critical infrastructure (see *supra*). The first Green Paper of November 2005[33] is the result of the Commission's and the Council's intention[34] to launch a European Program for the Protection of Critical Infrastructure (EPCIP), following the attacks in Madrid in 2004. This attempt soon came up against governance and coordination issues, as well as divergent views among Member States regarding the assessment of the threats to be considered (Lindström, Olsson, 2014). The Green Paper includes in the notion of critical infrastructure eleven economic and societal sectors, but these ambitions are reduced to the energy and transport sectors in the resulting directive[35]. Only thirteen European critical infrastructures were then identified by the Member States across the Union according to the obligations laid down by the Directive. The gas and electricity transmission networks were not included in the list. The directive has thus led to a strengthening of bilateral cooperation rather than genuine European cooperation, while the protection of these infrastructures ultimately falls to the Member States and to the owners and operators of these networks[36]. Despite a high degree of interconnection and interdependence, the EU has not instilled a real dynamic of cooperation regarding the security of its electricity networks.

The cyber threat is dealt with specifically in other programs or decorrelated agencies (European Union Agency for Network and Information Security) and the European institutional staff is too few on this subject to generate a real dynamic (Bossong, 2014). On the specific case of electricity grids, a thematic group on the protection of critical energy infrastructures was set up in 2010 by DG Energy and the Commission. Its biannual meetings, however, leave little room for the emergence of a true common dynamic. The Commission, through an evaluation of the EPCIP in 2013, pleaded for a more practical approach, which would also include the dominos effects that critical infrastructures of different natures (communication, energy, etc.) can have on each other (Bossong, 2014). Energy transmission networks are one of the four priority sectors identified.

In the absence of real European leadership at the institutional level, coordination actions are carried out by the network operators. Their European association, ENTSO-E, has been commissioned by the Commission to

---

[30] NERC, 2012, 2011 NERC Exercise Grid Security, After Action Report, Washington.

[31] NERC, 2014, Grid Security Exercise (GridEx II), After Action Report, Washington.

[32] NERC, Gridex III Public Report, 2015; NERC, GridEx IV Public Report, 2017. The reports are available online: https://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx

[33] Green Paper of 17 November 2005 on a European Program for Critical Infrastructure Protection COM (2005) 576.

[34] Commission européenne, COM(2004) 701 du 20 octobre 2004, Lutte contre le terrorisme : préparation et gestion des conséquences ; Commission européenne, COM(2004) 698 du 20 octobre 2004, Attaques terroristes : prévention, préparation et réponse.

[35] Council Directive 2008/114 / EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[36] European Commission, Commission staff working document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructure more secure, SWD(2013) 318, 2013.

prepare “network codes” common to the EU, that is, a set of common operating rules for network operators[37]. Even though the project is broader than just the security issue (it includes market rules, or technical prerequisites for connecting to the network of new works), one of these codes, “Emergency and Restoration”, is dedicated specifically to the issue of joint management of an event jeopardizing the stability of the network or the supply of consumers. It includes a system defense plan and synchronized network reconnection procedures[38].

In addition to the network codes, the European electricity network operators have also set up (especially following the 2006 blackout) Regional Safety Coordinators (RSCs) to monitor the network at a regional supra-state grid level (groups of neighboring States) and to inform the national network operators whose vision stops at their borders and allows for little coordination and optimization. While these initiatives by non-state European actors are necessary, they are not specifically calibrated to deal with cyber threats and physical attacks and they do not involve government or defense actors, who are primarily concerned in the event of an attack targeting these networks. Unlike the US threat response architecture, the EU has not made a direct link between industry players and defense officials. Compared to the American response system, the existing cooperations are much more the initiative of the industries, research centers or transmission system operators than the initiative of the EU institutions or governments. There are no structures or exercises bringing together all the actors involved in Europe (though the current dynamics aim towards this)[39]. There is also a structural and institutional separation between cyber threat / vulnerability management and physical threat / vulnerability that does not exist in US architecture.

Unlike the United States, which organizes exercises at the federal level, the EU has not put in place an integrated exercise at the community level. Communication channels between industrialists, network operators, national governments and European structures are weaker. There is, however, in the EU some ambitions for coordination such as the European Energy - Information Sharing & Analysis Center[40]. However, these initiatives never have a truly European dimension and they do not involve governments. Above all, the top down European approach separates the physical security of the network from cyber issues, treated separately, while the North American more bottom up approach starts from the network, to ask then the question of the nature of threats and possible responses. This same uncorrelated approach is used in NATO structures whose centers of excellence on energy and cyber cooperation (ENSEC COE and CCDCOE) are alternately present in different structures without displaying an integrated vision about power grid protection.

French actors have not officially participated in the various European-wide attempts mentioned above (for example SESAME or EE-ISAC). The French electricity grid is one of the most efficient in Europe and RTE, its manager, is a major and influential player in the European electricity landscape[41]. At the national level, PIRANET, the government plan devoted to state intervention in the event of a major IT crisis prepared and maintained by the National Agency for Information System Security (ANSSI) and the General Secretariat for National Defense and Security (SGDSN), took time to include the participation of the electricity transmission network. If PIRANET 2012 brought together operators of vital importance in the health, transport and communications sectors, it is not until 2016 that RTE, the manager of the French electricity network, evoked in its safety assessment a participation in the exercise which made it possible to “situate RTE's internal IT skills in terms of security and to establish links with the State services”[42].

## Conclusion

[37] Règlement (CE) N° 714/2009 du Parlement européen et du Conseil du 13 juillet 2009 sur les conditions d’accès au réseau pour les échanges transfrontaliers d’électricité.

[38] ENTSO-E, Network Code on Emergency and Restoration, 25 mars 2015.

[39] Nicolas Richet, Chief Information Officer, ENTSO-E – the European Network of Transmission System Operators for Electricity, Brussels, 11th of October 2018, “Cybersecurity in the Energy Sector – the European Perspective”.

[40] EE-ISAC seeks to improve the cyber security and resilience of power grids through information and data sharing. It is a joint initiative of four major European energy service providers (EDP, Enel, PES, Alliander), government and academic agencies, and technology providers.

[41] Interviews conducted within the European Network of European Transmission System Operators (ENTSO-E) in Brussels from January to July 2014.

[42] RTE, 2016, Bilan de sûreté.

The risks weighing on power networks have changed in the past decades. If the 20th century and its wars implied destruction and sabotage, the 21st century and the evolution of both conflict nature and energy management for capitalistic and globalized societies, bring a more complex nexus of hazards, vulnerabilities and resilience. Threats have become both cyber and physical and the two can combine, while the interconnection of networks and their opening to "smart" management and digital technologies have brought new vulnerabilities. A progressive awareness among American and European actors has led to the classification of power networks as "critical infrastructures" and the set up of specific strategies to protect them.

The comparison of the protection strategies of the American and European electricity transmission networks thus shows a double difference of approach. This difference is scalar. The United States has built an integrated institutional architecture based on seamless interaction and communication between scales. On the other hand, the European landscape is characterized by a multiplicity of initiatives at various scales without any real leadership or integrated vision of the problem (though recent trends show an awareness of the need for EU wide cooperation and information exchange). If these constructions seem *a priori* logical insofar as the United States is a nation-state while the European Union is an international organization with a weak political integration, two elements qualify this vision.

First, the United States has built its risk response strategy on a continental scale and not on a national scale, by integrating Canada and Mexico into its crisis exercises and by setting up an international regulatory authority (the North American Electric Reliability Corporation) as early as 1968. Conversely, the EU, which would be expected to act in this area of international cooperation, is paradoxically much more absent, and thus does not coordinate exercises at the Union level.

Secondly, from a technical point of view, the EU's integration policy has led to the gradual establishment of a network that is today highly interconnected and interdependent at a European scale, which makes it particularly sensitive to waterfall effects. Conversely, the United States has not pursued a policy of integration at the federal level and American networks are much less interconnected and interdependent. There is therefore a kind of paradox between the nature of these two entities and the policies they carry out on the technical level of infrastructures and on the organization of their protection.

The same difference arises at the sectoral level: the US vision integrates the management of vulnerabilities and physical and cyber threats into a single network-centric response plan, when the EU has separated the cyber and physical issues it manages through different channels. The operational efficiency of this European approach is questionable in a context of evolving vulnerability of these networks, marked by increasing interconnection and digital openness, partly linked to the energy transition policy. The question of how to manage the interdependencies resulting from the EU energy policy then arises from the point of view of the security of infrastructures essential to the functioning of European societies.

*Angélique Palle est chercheure à l'Institut de recherche stratégique de l'École militaire et chercheure associée à l'UMR Prodig. Elle travaille sur les questions d'approvisionnement et la protection des infrastructures énergétiques. Elle a soutenu en 2016 une thèse de géographie sur la construction de l'espace énergétique européen, suivie par un postdoc à l'Institut français du pétrole et des énergies nouvelles et l'Alliance nationale de coordination de la recherche sur l'énergie, sur l'intégration des énergies renouvelables variables aux réseaux d'électricité.*
*angelique.palle@gmail.com*

## References

Abramovici M., Bradley P., 2009, Integrated circuit security: new threats and solutions, in: Sheldon F., Peterson G., Krings A., Abercrombie R., Mili A. (Eds.), *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies* (CSIIRW '09), New York : ACM, DOI: 10.1145/1558607.1558671

Albertelli S., 2016, *Histoire du sabotage. De la CGT à la Résistance*, Paris : Perrin.

Baran P., 1964, *On distributed communications. Introduction to distributed communications networks, août 1964 - Rand Corporation*, Online archives.

Barrère J., 2002, *La genèse de l'Europe électrique, les logiques de l'interconnexion transnationale (début des années 1920 - fin des années 1950)*, mémoire de maîtrise sous la direction Christophe Bouneau, Université de Bordeaux -III. ed. Bordeaux.

Bongrain H., 1994, L'électricité au service de la Défense nationale, *in* : Lévy-Leboyer M., Morsel H. (dir.), *Histoire générale de l'électricité en France. Tome troisième*, Paris : Fayard, 556-576

Bossong R., 2014, The European Program for the Protection of Critical Infrastructure - meta-governing a new security problem?, *European Security*, 23: 2, p. 210-226. DOI: 10.1080 / 09662839.2013.856307

Galland J.-P., 2010, Critique de la notion d'infrastructure critique, *Flux*, 2010/3 (n°81), p. 6-18. DOI : 10.3917/flux.081.0006

Gleyze J.-F., 2005, *La vulnérabilité structurelle des réseaux de transport dans un contexte de risques*, Thèse de doctorat : géographie, sous la direction de Claude Grasland, Université Paris-Diderot - Paris VII.

Hoffmann, J., Caramanis, K., 2019, The Cost of Uncertainty in Curing Epidemics, in ACM SIGMETRICS Performance Evaluation Review 46(1), p.11-13, DOI: 10.1145/3308809.3308816

Kempf O., 2014, *Penser les réseaux. Une approche stratégique*, Paris : L'Harmattan.

Lagendijk V., 2008, *Electrifying Europe: The Power of Europe in the Construction of Electricity Networks*, Amsterdam: Amsterdam University Press.

Lindström M., Olsson S., 2014, The European Program for Critical Infrastructure Protection, in: Olsson S.(eds.), *Crisis Management in the European Union*, Berlin, Heidelberg: Springer, p 35-59. DOI: 10.1007/978-3-642-00697-5_3

Morsel H., 1994, Industrie électrique et défense en France lors des deux conflits mondiaux. Électricité, armement, défense, *Bulletin d'histoire de l'électricité*, nº 23, p. 7-17.

Palle A., 2016, Les dynamiques d'évolution des réseaux de transport d'électricité européens, des réseaux techniques entre croissance et décroissance, *Flux*, 2016/3 (N°105), p. 18-32. DOI:10.3917/flux.105.0018

Reghezza-Zitt M., Rufat S., 2015, *Resilience Imperative: Uncertainty, Risks and Disasters*, ISTE - Elsevier. DOI: 10.1016/C2015-0-01304-1

Reghezza M., Veyret Y., 2003, Aléas et risques dans l'analyse géographique, *Annales des mines*, n°40, p. 61-69.

Reghezza M., Veyret Y., 2006, Vulnérabilité et risques, l'approche récente de la vulnérabilité, *Responsabilité et environnement*, n°43, p.9-13.

**Abstract**

**Angélique Palle – Power networks as targets. Hazards, vulnerabilities and protection of power networks, from the Second World War to the 21st century asymmetric conflicts**

Power networks are "critical infrastructures" for industrialized western societies. As the electrification of energy uses grows, whereas the power sector is at the same time undergoing deep changes through energy transition, climate change mitigation or sustainable development dynamics, the evolution of their role and their increasing influence, calls for a renewed analysis of their exposure to risk. This paper explores the recent evolutions of this risk, brought by new hazards and vulnerabilities stemming from recent changes in these networks' environment. The point here is not to suggest technical resilience prospects, but to explore how the US and the EU have comparatively built a risk culture around these risks and how they manage them.

We will first analyze the recent evolution of the status of these networks that serve as a base for the entire economy and lifestyles of Western societies. From war goals for destruction in the twentieth century, they have become in the last ten years targets for physical sabotage (the Metcalf substation powering the Silicon Valley, in 2013) or cybernetic attacks (Ukrainian and Baltic cases). This analysis will then be confronted with the new vulnerabilities, induced by the integration of networks on a European scale which favors waterfall effects (case of the European blackout of 2006) and by the energy transition that opens networks to digital controls and makes them more vulnerable to cyberattacks. Thirdly, a comparative analysis of the American, European and French responses to these new risks weighing on the networks is proposed.

The analysis relies on various field and technical collaborations in EU and in the US, whereas most of the technical data stem from incident reports, security guidelines, stress test feedbacks and risk assessment from the network operators.

Keywords: Power networks, critical infrastructure, risk, European Union, United-States,

**Résumé**

**Angélique Palle – Les réseaux d'électricité vus comme cibles. Aléas, vulnérabilité et protection des réseaux de transport d'électricité, de la Seconde Guerre mondiale aux conflits asymétriques du 21e siècle**

Les réseaux électriques sont des "infrastructures critiques" pour les sociétés occidentales industrialisées. Alors que l'électrification des usages de l'énergie se développe et que le secteur de l'électricité subit en même temps de profondes mutations liées à la transition énergétique, l'atténuation du changement climatique ou la dynamique du développement durable, l'évolution du rôle l'influence croissante de ces réseaux appelle une analyse renouvelée de leur exposition aux risques. Cet article explore les évolutions récentes de ce risque, les nouveaux aléas et vulnérabilités liés aux changements récents de l'environnement de ces réseaux. Il ne s'agit pas ici de suggérer des perspectives de résilience technique, mais d'examiner comment les États-Unis et l'UE ont comparativement construit une culture du risque autour de ces risques et comment ils les gèrent.

L'article commence par explorer l'évolution récente du statut de ces réseaux qui servent de base à l'ensemble de l'économie et des modes de vie des sociétés occidentales. D'objectifs militaires au XXe siècle, ils sont devenus au cours des dix dernières années des cibles de sabotage physique (sous-station Metcalf qui alimente la Silicon Valley, en 2013) ou d'attaques cybernétiques (cas de l'Ukraine et des pays baltes). Cette analyse est ensuite confrontée aux nouvelles vulnérabilités de ces réseaux, induites par leur intégration à l'échelle européenne qui favorise les effets de cascade (cas du black-out européen de 2006) et par la transition énergétique qui les ouvre aux outils de contrôles numériques et les rend plus vulnérables aux cyberattaques. Enfin, une comparaison des réponses américaines, européennes et françaises à ces nouveaux risques est proposée.

L'analyse s'appuie sur des collaborations techniques et des terrains dans l'UE et aux États-Unis, tandis que la plupart des données techniques proviennent des rapports d'incidents, des lignes directrices en matière de sécurité, des retours d'expérience, des tests de résistance ou de l'évaluation des risques effectués par les opérateurs de réseau.

Mots-clés : Réseaux électriques, infrastructures critiques, risque, Union Européenne, Etats-Unis