Études de l'Ifri

CYBERSECURITY IN THE ENERGY SECTOR

A Comparative Analysis between Europe and the United States

Arnault BARICHELLA

February 2018

ifri Centre for Energy

Ifri is the principal independent center for research, information and debate on international questions in France. Created in 1979 by Thierry de Montbrial, Ifri is a non-profit, public-interest association. It defines its activities freely and regularly publishes its research, without being subject to any government supervision.

Ifri is associated with a number of political decision-makers and experts at the international level through studies and debates, which privilege an interdisciplinary approach.

This study is published as part of the ENERGEO project financed by the Conseil supérieur de la formation et de la recherche stratégiques (CSFRS).

ISBN: 978-2-36567-830-8

How to cite this publication:
Arnault Barichella, "Cybersecurity in the Energy Sector: A Comparative Analysis between Europe and the United States", *Études de l'Ifri*, Ifri, February 2018.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tel.: +33 (0)1 40 61 60 00 – Fax: +33 (0)1 40 61 60 60

Email: accueil@ifri.org

Website : Ifri.org

Author

Arnault Barichella is a doctoral candidate at Sciences Po Paris in the PhD program in Political Science. His research focuses on a comparative analysis of climate and energy policies in Europe and the United States.

Previously, he has worked at UNESCO and then at UNEP on the development of projects linked to energy efficiency, as well as sustainable consumption and production, in preparation for the COP21. He has also worked at the French Senate as a research assistant to prepare a 'Green Paper on Defense' that analyzes the impact of energy issues and environmental degradation on national security.

Arnault Barichella holds an MA in European Affairs from Sciences Po Paris, as well as a BA in Modern History from Oxford University.

Foreword

This policy paper has been prepared following a review of the relevant literature, as well as fifteen interviews with experts and professionals in the areas of energy and cybersecurity in Europe and the United States. The author would like to thank all those who agreed to be interviewed for their support and the information they provided on this sensitive subject. The interviews took place in the United States and Europe, with experts drawn from as wide a sample as possible to represent the relevant actors in both the public and private sectors. Since the individuals who agreed to be interviewed have asked to remain anonymous, the information that derives from these interviews, and which was used to prepare this policy paper, has not been attributed.

Executive summary

The acceleration of the digitization of energy infrastructure has brought many economic benefits, including greater efficiency in the rationalization of energy consumption. However, this has also increased the risk of cyberattacks, where malicious software is able to take advantage of the increasing digitization of energy equipment. The recent cyberattacks that have targeted critical infrastructure in Ukraine highlight that the threat is real and growing. Vulnerability is not restricted to infrastructure located within the European Union (EU) or the United States (US): the cyberattacks that recently hit Ukraine spread to many Western firms through their subsidiaries, underlining the danger of contagion.

As a result, over the last few years, the EU and the US have gradually sought to put in place a series of policies and rules to protect energy infrastructure from cyber threats. The American and European approaches in this area present many differences. The United States has favored a strategy of 'security in depth' with strict and detailed regulations in specific sectors, which are implemented by institutions possessing coercive powers. By contrast, the EU has adopted a more flexible and exhaustive approach covering a wide range of issues, leaving an important margin of maneuver for member states in the implementation of norms. Nevertheless, these approaches are potentially complementary in that the strengths of the American system can serve as a model to improve certain weaknesses in the European approach, and vice versa, since the US could also learn from the EU in a number of areas.

Indeed, the American model is in advance compared to the EU in terms of the development of precise and detailed norms on cybersecurity, as well as for the implementation of these norms. Only a handful of EU member states, including France, have an equivalent level of norms, and Europe suffers from inadequacies both at the EU level and at the national level. Nevertheless, the US can learn from the EU in other areas, such as the protection of privacy and personal data, cybersecurity for renewable energies and low carbon technologies, as well as the protection of the electricity network at the level of distribution. Moreover, California and France present a number of relevant specificities regarding cybersecurity.

This is why it is essential to enhance transatlantic cooperation in order to allow the EU and the US to learn from one another's cybersecurity frameworks. This should take place at different levels, including reinforcing bilateral cooperation between governments, better cooperation through multilateral organizations such as NATO or the G7, along with stronger public-private partnerships. The objective would be to encourage a harmonization of norms between the EU and the US in order to gradually put in place common transatlantic cybersecurity standards. It is important to note that President Trump has demonstrated an interest in cybersecurity issues, as he has chosen to reinforce the policies of his predecessor in this area. Thus, in spite of current differences between the EU and the US on many issues, cybersecurity represents one area where there exists a real opportunity to deepen transatlantic cooperation in the years to come.

As a result, common transatlantic standards could then become rigorous international cybersecurity norms, helping to reduce the risks of contagion. There is also an important economic dimension, where any delay from the EU regarding cybersecurity may decrease the competitiveness of specialized European firms vis-à-vis their American counterparts. This could lead to potentially significant losses in a growing market that increasingly represents hundreds of millions of euros in investment and thousands of jobs per year for the energy sector within the EU.

Table of contents

Introduction

As digitization accelerates in our societies, cybersecurity has become an increasingly important issue that touches on nearly all sectors and activities. The energy sector possesses its own particular characteristics that require specific regulations, which are complementary but often different from those in other sectors. Indeed, information and communication technologies (ICTs) have only slowly been integrated into energy infrastructure. This is mostly due to the length of investment cycles in this sector, a factor that has delayed its digitization. Nevertheless, the need to rationalize production, distribution and consumption in order to manage an increasing amount of data, along with the objective of facilitating communication between different sites and equipment, have all contributed to the gradual deployment of ICTs in energy infrastructure. This digitization has allowed for important efficiency gains by optimizing the supply chain thanks to the analysis of complex data and remote controlling. The consumer now benefits from more personalized services, enabling a better management of energy consumption with less waste. In spite of these advantages, however, the deployment of ICTs in the energy industry has also had the consequence of considerably increasing the risk of cyberattacks. Indeed, the energy sector has gone from relatively isolated and protected industrial systems to an open network relying on technologies that are highly interconnected with the Internet and with business networks. Moreover, due to the length of investment cycles, the infrastructure is often aged, and much of the equipment will remain operational for several more decades. The latter was designed at a time when cyber risks were under-developed, and thus cyberdefense has not been integrated into its functionality, which makes the equipment vulnerable to hacking. Likewise, protection software borrowed from the IT sector is not necessarily transferable to energy infrastructure.

This type of vulnerability has exposed the energy industry to a growing number of cyberattacks over the last few years. Cybersecurity includes both protection from computer viruses intended to cause physical and material damage, as well as from hacking and theft of personal data for commercial profit. Indeed, industrial espionage and cybercriminality are among the principal causes of cyberattacks, and represent a violation of privacy. In addition to companies spying on each other and from one country to the other in order to gain a competitive advantage, criminal groups are also

increasingly relying on malicious software to achieve their goals. Moreover, the political dimension has also become a major factor over the last few years. In this regard, the risks looming over the energy sector were revealed in 2010 with the discovery of the *Stuxnet* virus, which had infected Iran's *Natanz* uranium enrichment complex. *Stuxnet* highlighted that cyberattacks could also be related to geopolitical factors and conducted by nation states.[1]

The strategically critical role of the energy industry in the national economy and for all vital State functions (defense, communications, and healthcare, for example) have turned the industry into an increasingly privileged target for cyberattacks, often in relation to geopolitical confrontations between great powers. This is partly due to the fact that it is often difficult to attribute with precision the responsibility for a cyberattack, which allows a State to rely on mass spying or to cause major damage while remaining undetected.[2] Thus, even though Russia is a prime suspect, it has not yet been possible to accurately attribute the responsibility for a series of cyberattacks that have recently hit Ukraine.[3] This includes the *Black Energy* virus in December 2015, which managed to disconnect thirty Ukrainian power stations, affecting more than two hundred thousand people in eight regions for several hours. In May 2017, Ukraine was once again hit by a cyberattack with the *XData* virus, which served as a precursor for a far more devastating attack one month later with the *NotPetya* virus. According to the latest estimates, the latter infected more than 18% of Ukraine's energy companies, and in total more than 30% of all computer systems across the country. Many Western firms that have commercial links with Ukraine were affected by the virus, including the French group *Saint-Gobin* and the Danish transporter *Maersk,* as well as their sub-contractors. Indeed, large international groups are particularly vulnerable through their subsidiaries, which are spread across many countries around the world.[4] The EU and the United States had already been hit earlier that year by the global propagation of the *WannaCry* virus on May 12th, which impacted more than "200,000 victims" in 150 countries according to Europol, with significant damage across many different sectors.

1. Several subsequent investigations have made it possible to determine that the level of sophistication of the *Stuxnet* virus required advanced technology and funding, and had probably been supported by a powerful country. See: Desarnaud G., "Cyber Attacks and Energy Infrastructures: Anticipating Risks", *Études de l'Ifri*, Ifri, January 2017, available at: www.ifri.org.
2. See: Lindsay J. R., "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack", *Journal of Cybersecurity*, Volume 1, Issue 1, 1 September 2015, pp. 53–67.
3. See: *Global Cybersecurity Summit 2017*, which was held in Kiev (Ukraine) on the 14-15 June 2017, available at: https://gcs17.com.
4. Guiton A., "Enquête : Les cobayes de la cyberguerre", *Libération*, 28 July 2017, available at: www.liberation.fr.

In order to manage these real and growing threats, the United States and the EU have progressively put in place a number of regulations, laws and institutions in order to protect the energy sector from cyberattacks. The research and interviews conducted for this policy paper have highlighted several important differences in their respective approaches. Indeed, the US has adopted a strategy of 'security in depth' that focuses on strict and detailed regulations in specific sectors, which are implemented by institutions possessing coercive powers. By contrast, the EU has chosen a more flexible and exhaustive strategy, which favors the protection of a wide range of different sectors such as electricity distribution, low carbon technologies, as well as privacy and personal data. Thus, the European and American approaches regarding cybersecurity appear to be intrinsically complementary, with strong potential to reinforce transatlantic cooperation. The first part of this paper will analyze what the EU can learn from the US regarding cybersecurity in the energy sector. The second part will then examine what the US can learn from the European approach. California and France will be presented as examples of a US state and an EU country with pertinent specificities in terms of cybersecurity. The third part of this paper will propose solutions to reinforce transatlantic cooperation so that the EU and the US may develop common international standards for cybersecurity in the energy sector.

The issue of protecting nuclear infrastructure from cyber risks is of fundamental importance. For many years, this specific area has been regulated by the International Atomic Energy Agency (IAEA), the global governance authority for civil nuclear energy, and will not form part of the framework for this policy paper.[5]

5. IAEA, "Computer Security at Nuclear Facilities", Security Series No. 17: Technical Guidance Reference Manual, 2011.

Comparative perspectives: what the European Union can learn from the United States

The development of strict, detailed and comprehensive cybersecuity norms

The terrorist attacks on September the 11th 2001 accelerated the development of comprehensive and detailed cybersecurity norms in the United States. American authorities gradually came to realize the key strategic importance of the energy sector. In 2005, the US Congress ratified the Energy Policy Act, which gave the Federal Regulatory Commission (FERC) responsibility to designate an entity (the 'Electric Reliability Organization', ERO) to establish security standards for the electricity network at the federal level. The 'North American Electric Reliability Corporation' (NERC), a private organization,[6] was chosen as the ERO for the United States as a whole and placed under the supervision of the FERC. The NERC has developed a series of cybersecurity norms, targeting the production and transmission sections of the power grid (the 'Bulk Power System', BPS). Compiled under the name of Critical Infrastructure Protection Standards, or 'NERC-CIPs', the FERC approved the first version of the NERC-CIPs in January 2008. They are among the most detailed and comprehensive cybersecurity standards in the world, and are mandatory for all 3000 electric utilities in the United States. This includes precise measures covering, for example, the security of management controls, personnel and training, the physical security of the BPS, as well as recovery plans for computer systems in the event of a cyberattack. Moreover, the NERC-CIPs have been updated on a regular basis in order to keep-up with the rapid evolution of cyberthreats. For instance, the FERC approved the 5th version in 2013 and the 6th version in 2016, bringing noticeable improvements. During his second mandate, President Obama signed one Executive Order (EO)[7] and two Presidential Policy Directives (PPD),[8] in order to bypass

6. The NERC has a mandate to ensure the security of the electricity grid not only in the United States, but also in parts of Canada and Mexico.
7. *Executive Order* 13636, "Improving Critical Infrastructure Cybersecurity" (12/02/2013).
8. *Presidential Policy Directive* 21, "Critical Infrastructure Security and Resilience" (12/02/2013) and *Presidential Policy Directive* 41, "United States Cyber Incident Coordination" (26/07/2016).

Congress, which had blocked the ratification of the GRID Act[9] in 2012. Moreover, it is important to underline that cybersecurity represents a subject where the current American President has chosen to continue the policies of his predecessor. Indeed, Donald Trump has demonstrated a notable interest in cybersecurity issues, having already signed an EO that enhances and consolidates the measures taken by Obama, which includes a review of all federal norms in order to identify necessary updates.[10]

Objectives of the NERC-CIP standards (Versions 5 and 6)

Number	NERC-CIP Standards (Versions 5 and 6)	Objectives	Date of entry into force
CIP-002 5.1a	BES Cyber System Categorization	Categorize different computer systems in order to identify vulnerabilities in the electricity network and find appropriate measures	12/2016
CIP-003-6	Security Management Controls	Establish responsibility and reinforce control mechanisms for the management of cybersecurity incidents in the electricity network	7/2016
CIP-004-6	Personnel and training	Minimize the risks of accidents linked to human error by reinforcing personnel training for cybersecurity	7/2016
CIP-005-5	Electronic Security Perimeter	Manage a secure access to the electricity network by establishing an electronic security perimeter around infrastructures	7/2016
CIP-006-6	Physical Security of BES Cyber Systems	Protect and manage physical access to computer systems by	7/2016

9. O'Keefe E. and Nakashima E., "Cybersecurity Bill Fails in Senate", *The Washington Post*, 2 August 2012, available at: www.washingtonpost.com.
10. *Executive Order* 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure".

		defining a security plan for the entire electricity network	
CIP-007-6	System Security Management	Reinforce the security system by defining technical, operational and procedural requirements for the electricity network	7/2016
CIP-008-5	Incident Reporting and Response Planning	Put in place procedures for the signaling of cybersecurity incidents and the planning of interventions for the electricity network	7/2016
CIP-009-6	Recovery Systems for BES Cyber Systems	Define plans for the recuperation of computer systems in the event of a cyberattack on the electricity network	7/2016
CIP-010-2	Configuration Change Management and Vulnerability Assessments	Evaluate the vulnerabilities of computer systems during software updates and changes in network configuration	7/2016
CIP-011-2	Information protection	Put in place measures to protect computer systems against the theft and hacking of data needed for the proper functioning of the electricity network	7/2016
CIP-014-2	Physical Security	Identify critical infrastructure within the electricity network and implement measures to ensure protection from physical attacks	10/2015

Although the EU began to address cybersecurity issues at approximately the same time as the US, its policies lack the same level of precision and detail compared to American legislation. The 2006 European Program for Critical Infrastructure Protection (EPCIP), as well as the 2008 European Critical Infrastructure Directive (ECI), leave a wide margin of maneuver for member states and are limited by the fact that they define only general and imprecise criteria for the protection of critical infrastructure.

The EU Cybersecurity Strategy, adopted in February 2013, establishes a list of strategic priorities comprising critical infrastructure, which includes the energy sector. Nevertheless, the document focuses on other sectors mainly related to cybercriminality and the Common Security and Defense Policy (CSDP); it does not propose any concrete measures, but focuses instead on general strategic axes. Moreover, the Directive on the Security of Network Information Systems (NIS), adopted in June 2016, sets a basis for the development of European norms by establishing common criteria for 'operators of essential services' (OES).[11] The new Cybersecurity Package, proposed by the European Commission in September 2017, contains practical advice regarding the implementation of the NIS Directive and for the interpretation of certain of its clauses.[12] These provisions were later confirmed during the Digital Summit that took place in Tallinn on 29 September 2017 under the Estonian Presidency of the Council of the European Union. In spite of this, member states have been left with the responsibility to define the detailed content of norms, with each country being entrusted to develop its own national cybersecurity strategy. Therefore, the NIS Directive may not be sufficiently precise because it establishes only general criteria regarding what constitutes an OES and what type of security measures should be implemented, including for the prevention and management of cyber risks. Thus far, the result has been the development of a multi-speed Europe, with important differences between countries regarding the development of cybersecurity norms.

According to an extensive study by the Software Alliance (BSA), European norms for cybersecurity are highly variable within the EU. While most member states have put in place a national cybersecurity strategy, several such as Bulgaria, Greece, Denmark, Ireland and Sweden have still not done so. Moreover, countries such as Croatia, Latvia, Luxembourg and Portugal have not developed national plans for the protection of critical infrastructure, while others such as Belgium, Italy and Slovakia lack legislation prescribing at least one annual cybersecurity audit.[13] This situation is problematic because European energy infrastructures are highly interconnected. Member states with the least developed cybersecurity norms constitute weak links, enabling malicious software to penetrate and then spread to the entire network. As a result, it is essential to reinforce the NIS Directive with more detailed, in-depth norms, and the EU could rely on

11. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Available at: http://eur-lex.europa.eu.

12. European Commission, *New Cybersecurity Package*, September 2017, available at: https://ec.europa.eu.

13. BSA/The Software Alliance, *EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace*, January 2015, available at: http://cybersecurity.bsa.org.

the American NERC-CIPs as a model. Although it would be impossible to copy the American federal system, the EU can nonetheless learn from the US regarding the elaboration of more precise and comprehensive norms for cybersecurity. What is more, the development of specific and frequently updated regulations for the electricity network, instead of for critical infrastructure in general as prescribed by the NIS Directive, would allow for a higher level of detail and precision. The EU could adopt a new legislative initiative that would integrate such norms, but this would need to be done under the format of a Regulation. Indeed, unlike Directives that need to be transposed into national law, Regulations are directly applicable without the need for transposition measures and are applied in a simultaneous and uniform way to all member states, thus reducing the risk of differentiated norms across EU countries.

Comparison between European and American cybersecurity norms (in chronological order, color blue for the UE and white for the US)

Date of ratification	Name of the law or regulation	Summary and principal clauses
08/2005	*US Energy Policy Act*	Gives a mandate to the FERC to designate an *Electric Reliability Organization* (ERO) in order to put in place mandatory security standards for the electricity network
01/2006	EU Security of Supply Directive (SOS)	Establishes a series of measures to secure the EU's electricity supply, as well as the proper functioning of the internal electricity market, without referring specifically to cybersecurity
12/2006	European Program for Critical Infrastructure Protection (EPCIP)	Establishes a general inter-sectorial framework for the security of critical infrastructure, which includes cybersecurity, terrorism, organized crime and natural catastrophes
12/2007	*US Energy Independence and Security Act*	Gives a mandate to the 'National Institute of Standards and Technology' (NIST) in order to put in place security standards for smart grids
12/2008	European Critical Infrastructure Directive (ECI)	Establishes general criteria to identify and protect critical infrastructure, including in terms of cybersecurity, which apply to both the energy and transport sectors

10/2010	EU Security of Gas Supply Regulation	Establishes a series of measures to secure the EU's gas supply. An updated version that includes cybersecurity was adopted in April 2017 and will come into force in the near future.
02/2013	*US Executive Order 13636 "Improving Critical Infrastructure Cybersecurity"*	Orders the NIST to put in place a cybersecurity framework to allow for the secure development of the smart grid. The result has been the launching of the 'NIST Framework' which, even if not binding but voluntary, has been adopted by most US firms
02/2013	*US Presidential Policy Directive 21 "Critical Infrastructure Security and Resilience"*	Reinforces the control of federal agencies over critical infrastructure, including in the energy sector
02/2013	EU Cyber Security Strategy	Establishes a list of strategic priorities for cybersecurity in the EU that refers to critical infrastructure, including the energy sector
12/2015	*Fix America's Surface Transportation Act (FAST Act)*	Even though this law focuses mostly on the transport sector, it also increases the powers of the Secretary of Energy to manage cyberattacks on the power grid
06/2016	EU Directive on the Security of Network and Information Systems (NIS)	Establishes foundations for the development of European cybersecurity norms by defining common criteria for 'operators of essential services', as well as the necessary policies to be implemented, including for the prevention and management of risks
07/2016	*US Presidential Policy Directive 41 "United States Cyber Incident Coordination"*	Reinforces the coordination of federal institutions charged with the development of national cybersecurity standards, including FERC, NERC and the Department of Energy
05/2017	*US Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"*	Orders the Secretary of Energy, in consultation with other federal agencies, to study the resistance of the electricity network against cyberattacks in order to identify necessary updates

09/2017	Cybersecurity Package, proposed by the European Commission	Contains practical advice for implementation of the NIS Directive. It also seeks to reinforce ENISA's competences by giving it a permanent mandate, in addition to establishing a European certification system in order to create an internal market for cybersecurity

An effective system for the implementation of cybersecurity norms

The United States has also successfully developed a relatively advanced system with respect to implementation of cybersecurity norms, another area where the EU could learn from the American model. Indeed, the NERC possesses a number of binding mechanisms to verify that electric utilities are in conformity with the NERC-CIPs. Firstly, it can impose fines that can reach up to one million dollars per day until standards are properly implemented. The NERC has recently taken the decision to increase the level of fines in order to dissuade firms from breaching the rules; for example, it imposed two fines in 2016 that reached 1.1 and 1.7 million dollars.[14] According to one of the experts interviewed for this paper, this represents an extremely effective policy to reduce fraud, since utilities usually prefer to conform to the norms rather than face such high fines. The NERC also possesses specialized intervention teams whose mission is to inspect a number of utilities each year in order to verify the implementation of security norms.

Moreover, the NERC has developed an alert system ('NERC Alerts') that makes it possible to simultaneously inform all utilities in the US of an imminent cyber threat. These NERC Alerts help to verify utility coordination and response time, which makes it easier to identify those that do not sufficiently respect the rules, as well as the necessary updates to install. The NERC has emitted 41 alerts since 2009, including two high-level alerts in 2016, the first following the cyberattacks in Ukraine, and the second for malicious software targeting the Internet of Things.[15] Moreover, the NERC also organizes an extensive conference (the Grid Security Conference or 'GridSecCon') each year that brings together cybersecurity experts from both the public sector and industry. The GridSecCon allows all relevant stakeholders to exchange technical information so that cybersecurity norms

14. Fallon R. and Lazaroff M., *NERC Increasing Penalties for Fundamentally Failing to Comply with Cyber Standards*, Cozen O'Connor, November 2016, available at: www.lexology.com.
15. Following this, NERC published, in cooperation with E-ISAC, a document to reinforce implementation of cybersecurity norms for utilities in relation to the Internet of Things (*Internet of Things DDoS White Paper*).

can be implemented in a synchronized manner. Finally, the NERC organizes a large-scale exercise every two years that simulates a cyberattack on the power grid (the Grid Security and Emergency Response Exercise or 'GridEx') in collaboration with federal agencies and local governments, as well as the private sector. The latest exercise of this kind (GridEx IV) took place on 15-16 November 2017 with nearly 7000 participants from 450 different organizations; this allowed for a real time test of the effectiveness of cybersecurity strategies and identification of possible upgrades. In order to carry out its mission, NERC possesses a substantial budget ($69.6 million in 2017) and a staff of approximately 190 full time employees, together with many consultants and sub-contractors.[16]

Institutional challenges for the European cybersecurity system

At the level of the EU, there is no equivalent regarding the implementation of cybersecurity norms. The European Union Agency for Network and Information Security (ENISA) was established in 2004. It is based at Heraklion in Greece, and its mandate was enhanced by the EU in 2013.[17] In the new Cybersecurity Package proposed in September 2017, the European Commission seeks to to reform ENISA by giving it a permanent mandate, as well as reinforcing several of its competences so that it is better able to support member states. This includes assisting with implementation of the NIS Directive, which was reaffirmed during the Digital Summit in Tallinn in September 2017. Despite these advances however, ENISA's role remains limited to advising member states, collecting and analyzing data, promoting crisis management methods, and encouraging the exchange of best practices. The Agency lacks any form of coercive power, and its resources are far below those of the NERC.[18] For example, ENISA had a 2017 budget of €11.2 million (compared to $69.6 million for NERC), and a team of 84 full time employees (compared to 190 plus subcontractors for NERC).[19]

16. Given the extent of its mandate that covers a large section of North America, the NERC's full time staff may appear to be below what could be expected. This is due to the fact that NERC, as a private organization, externalizes and sub-contracts an important part of its activities. See: *NERC 2017 Business Plan and Budget, Final Draft, Finance and Audit Committee Meeting,* August 2016, available at: www.nerc.com.

17. Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA). This Regulation renewed ENISA's mandate for seven years and enhanced its responsibilities, including in the fight against cybercriminality.

18. Another noticeable difference between the EU and the US is that ENISA is a public institution, whereas NERC is a private organization under the supervision of a federal agency (FERC).

19. ENISA, *Statement of Estimates 2017* (Budget 2017), 2017. ENISA, *Multi-Annual Staff Policy Plan 2016-2018*, October 2015. The New Cybersecurity Package proposed by the European

Moreover, the NIS Directive obliges each member state to create its own national cyber alert center (a Computer Security Incident Response Team or 'CSIRT'), with a mandate to ensure that 'operators of essential services' comply with cybersrcurity norms. The Directive also provides for the creation of a network composed of all national CSIRTs, as well as a 'Cooperation Group' involving the European Commission and competent national institutions, in order to encourage information sharing. Nevertheless, neither the CSIRT network nor the Cooperation Group have any coercive powers to ensure the implementation of cybersecurity norms; this responsibility has been left to national CSIRTs. Therefore, it is member states that must decide which competences to attribute to their national CSIRTs and how they wish to organize the verification of standards. Even though the provisions of the NIS Directive must be adopted by May 2018, the result will likely be the development of a multi-speed Europe, where the effectiveness of national CSIRTs will vary from one country to the other. This situation is potentially dangerous, since member states lacking a sufficiently binding CSIRT risk becoming weak links that will increase the vulnerability of the European network as a whole. Already, important differences between member states have become apparent regarding the implementation of cybersecurity norms.[20] Furthermore, there is also an economic dimension, since any delay on the part of the EU in terms of cybersecurity protection risks decreasing the competitiveness of specialized European firms when compared to US firms, representing potentially significant financial losses.

Although it would be problematic to recreate a European organization like the American NERC, the EU could nonetheless learn from it to reinforce current institutions, or create new ones with additional competences. The main obstacle has been the reluctance of a number of member states to share sensitive information with other European countries. Nevertheless, the recent cyberattacks in Ukraine, which spread to many member states and caused substantial damage, have underlined the danger that weak leaks represent. As a result, it would be beneficial to create one principal CSIRT at the EU level with sufficient powers to coordinate national CSIRTs, or to reinforce both the resources (in terms of budget and staff) and the

Commission in September 2017 seeks to enhance ENISA's resources by doubling its budget to €22 million and by increasing its staff to 120 full time employees by 2021. While these are positive developments, they remain insufficient, especially when compared to the financial and logistical means of the American NERC, which continue to increase on a regular basis.

20. According to a study by the Software Alliance (BSA), even though most member states have already put in place a national CSIRT, several such as Cyprus and Ireland have still not established a platform for the centralization of data and reporting on cybersecurity incidents. Moreover, a majority of EU countries, including Belgium, Finland, Ireland and Slovenia, have not developed a national structure with sufficient competences and resources to manage cybersecurity incidents. See: BSA/The Software Alliance, *EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace*, January 2015, available at: http://cybersecurity.bsa.org.

competences of ENISA. This could include the possibility of imposing fines at the European level for non-compliance with cybersecurity rules, the notification of incidents and better information sharing between public and private actors, as well as the establishment of regular inspections in member states (competences which the EU has already acquired in other areas).

Moreover, if member states refuse to transfer these powers, it would still be possible for ENISA, or the CSIRT network, to develop a cyber alert system at the European level for firms and institutions in the energy sector based on the model of the NERC Alerts. Although the EU has already put in place a similar framework (CERT-EU), the latter works mainly in relation with other EU agencies and institutions. The CERT-EU does not focus specifically on the energy sector, and does not possess the same type of direct and regular contact with all electric utilities and firms in the sector like the American NERC. For European countries, this would not involve a transfer of national sovereignty and could contribute to reinforcing the harmonization of norms and information sharing between national CSIRTs. Furthermore, although ENISA also organizes a cybersecurity exercise every two years, it is less developed than the American GridEx and does not focus specifically on the energy sector. The fourth and latest cybersecurity exercise, 'Cyber Europe 2016', was organized by ENISA in April and October 2016. It brought together approximately 1000 participants (far less than the 7000 participants in GridEx IV) coming from different sectors, including telecommunication operators, ICT companies, as well as several energy firms.[21] One possibility would be for the EU to regularly participate in the GridEx in order to learn from American methods, which would help to improve cybersecurity exercises in Europe. Likewise, ENISA could also enlarge its exercises to include neighboring countries such as Ukraine that are members of the Energy Community, and which are linked to the European internal energy market.[22]

21. ENISA, *Cyber Europe 2016: After Action Report*, June 2017, available at: www.enisa.europa.eu.
22. European Commission, *Energy Community*, available at: https://ec.europa.eu.

Comparison of the implementation of cybersecurity norms between the EU and the US (color blue for the UE and white for the US)

Institution or competence	Role and objectives
NERC Fines	NERC may impose fines that can reach up to one million dollars per day until standards are properly implemented
NERC Intervention Teams	NERC sends intervention teams to inspect a certain number of utilities each year in order to verify the implementation of norms
NERC Alerts	NERC has an alert system that helps to inform all utilities in a synchronized manner of an imminent cyber risk
Grid Security Conference	NERC holds a conference each year that brings together cybersecurity experts from both industry and the public sector to exchange technical information
Grid Security and Emergency Response Exercise	NERC organizes every two years a large-scale exercise that simulates a cyberattack on the electricity network in collaboration with federal and local institutions, as well as the private sector
ENISA	Its role is to advise member states, gather and analyze data, promote risk management methods, as well as encourage the sharing of best practices
National CSIRTs	National alert systems for member states, whose mission is to ensure that 'operators of essential services' respect cybersecurity standards
CSIRT Network	Its mission is to develop trust between member states in order to encourage information sharing and cooperation between national CSIRTs
Cooperation Group	Its function is to reinforce collaboration between member states and the European Commission regarding cybersecurity
Cyber Europe Exercise	ENISA organizes cybersecurity exercises every two years that bring together participants coming from different sectors, including the energy sector

The Californian model for cybersecurity

California is probably the most advanced US state on cybersecurity issues. The EU could learn from the Californian model, especially regarding implementation of the NIS Directive, which stipulates that each member state is required to establish a national cybersecurity center (CSIRT). California's Governor Jerry Brown took the initiative in August 2015 to create the Cyber Security Integration Center ('Cal-CSIC'), which has the same functions as European CSIRTs regarding the management and prevention of cybersecurity incidents on critical infrastructure. Nevertheless, the Cal-CSIC also possesses competences in other domains, which reflects a more comprehensive approach to cybersecurity that could serve as a model for European CSIRTs. Indeed, the mandate of the Cal-CSIC also covers the development of new technologies and digital systems to reinforce cyberdefense mechanisms. This includes support for scientific and technical research, as well as close partnerships with the private sector in order to identify the best technologies and computer software. Moreover, the Cal-CSIC is also responsible for verifying the protection of privacy and personal data for consumers in relation to new digital technologies, including for smart meters. Within the EU, these functions are spread across a variety of sectors with a multitude of different institutions. Member states have specific institutions to ensure privacy protection; for example, France has put in place a 'National Commission on Informatics and Liberty' (*Commission nationale de l'informatique et des libertés*, CNIL). Furthermore, it is the European Commission that is charged with supporting scientific and technical research in this area, through frameworks such as the 'Horizon 2020' program. Nevertheless, such a division of competences could be problematic in that it may hamper effective coordination between intricately connected domains. Therefore, the Cal-CSIC's comprehensive approach regarding cybersecurity could serve as a model to reinforce centralization between the various institutions in European states; for example, this may lead to a more effective collaboration between the CNIL and the CSIRT in a country such as France.

A second point on which California could serve as an example for the EU concerns the protection of personal data in the energy sector. The General Data Protection Regulation (GDPR), adopted in April 2016, represents the main European legislation regarding the protection of personal data. The GDPR is general in its scope, which means that it applies to most sectors, including the energy sector. California's particularity is that it possesses laws that are designed to protect personal data specifically in the energy sector, which also includes smart meters. For example, the 'Privacy for Customer Electrical or Natural Gas Usage Data Law' came into effect in

January 2014.[23] This law prohibits any private entity from sharing or disclosing information concerning an individual's consumption of electricity or natural gas without having obtained explicit consent.[24] It also contains specific clauses on smart meters, and imposes strict rules for firms that manage this type of technology. This comprises an obligation to rely on advanced cybersecurity mechanisms to protect data that is collected from smart meters, including the systematic encryption of personal data. By contrast, even though the GDPR seeks to put in place concrete and ambitious measures in this area, the latter do not contain any specific clauses for the energy sector. According to one of the experts interviewed for this paper, the GDPR's general character could hamper its ability to protect personal data collected by smart meters. Indeed, the technicality of these new digital technologies and the important risks they introduce in relation to cybersecurity render it necessary to implement specific and targeted legislation in order to guarantee an adequate level of protection for privacy at the individual level.

What France could learn from the American model

France is a country that is relatively advanced regarding cybersecurity, even when compared to the United States. The 2008 White Paper on Defense and National Security (*Livre blanc de la défense et la sécurité nationale*) contributed to establishing an autonomous structure to ensure the cybersecurity of information systems. Created in 2009, the National Cybersecurity Agency of France (*Agence nationale de la sécurité des systèmes d'informations*, ANSSI) is today amongst the most developed agencies in the field, with a budget of approximately €80 millions (slightly more than NERC's budget which is close to $70 millions[25]). The ANSSI's mission has been defined around several strategic axes, including detecting cyber attacks, preventing threats, advising administrations and operators, as well as regularly informing firms and the public about cyber issues. Its competences were reinforced following the implementation of France's National Cybersecurity Strategy in 2011 (*Stratégie de la France en matière*

23. California Legislative Information, *AB-1274 Privacy: Customer Electrical or Natural Gas Usage Data*, October 2013, available at: https://leginfo.legislature.ca.gov.

24. This law also requires that energy firms reveal to consumers how their personal data is being processed and to whom it may have been transferred, obliging firms to implement measures to prevent data theft and hacking.

25. This is partly due to the fact that the NERC focuses only on the energy sector, whereas the ANSSI has a much broader mandate that covers the security of all information systems, which requires a bigger budget.

de défense et de sécurité des systèmes d'information).[26] Moreover, the 2013 version of the White Paper on Defense and National Security underlined the importance of ensuring cybersecurity for 'operators of vital importance' ('OVI'). France's Military Programming Law (*Loi de programmation militaire*), adopted in 2013, established the judicial foundations for a national cybersecurity policy by setting strict rules for more than 200 entities identified as constituting OVIs.[27] Although the full list is classified,[28] it mostly includes firms, factories, operators and institutions "for which any breach to its security or to its functioning would risk significantly decreasing national military or economic potential, as well as the security or survival of the Nation".[29]

Moreover, the 2015 Decree regarding the security of information systems for OVIs has helped to clarify the rules regarding detection of cyber incidents, modalities for declaring such incidents, as well as the necessary provisions for prevention and protection from these threats.[30] This ambitious framework has been completed by a revised version of France's National Cybersecurity Strategy (*Stratégie nationale pour la sécurité du numérique*), presented by the ANSSI in Fall 2015.[31] Furthermore, France was the first country to publish sectorial decrees for its OVIs in August 2016 (*arrêtés sectoriels*), containing a list of precise, detailed and mandatory policies for firms aimed at protecting their information systems.[32] The sectorial decrees contain measures that are adapted to the specific context of different sectors, including the energy sector, with strict rules for OVIs concerning hydrocarbons,[33] gas,[34] and electricity.[35] This includes the obligation for firms to provide the ANSSI with a list of their information systems of vital importance within three months, the establishment of a policy for the security of information systems, the mapping of existing systems, as well as a duty to plan ahead for the update of any new software.

26. ANSSI, *French National Cybersecurity Strategy*, 2011, available at: www.ssi.gouv.fr.
27. Law n° 2013-1168 on the 18th of December 2013 regarding military programming for the years 2014 up to 2019, available at: www.legifrance.gouv.fr.
28. The list of OVIs was previously established by the Decree n° 2006-212 on the 23rd of February 2006 regarding security for activities of vital importance, available at: www.legifrance.gouv.fr.
29. Article L1332-6-1 of the French Defense Code.
30. Decree n° 2015-351 on the 27th of March 2015 relating to the security of information systems for operators of vital importance, available at: www.legifrance.gouv.fr.
31. ANSSI, *National Cybersecurity Strategy*, 2015, available at: www.ssi.gouv.fr.
32. ANSSI, *Cybersecurity for OVIs: publication of a new wave of sectorial decrees*, 2016, available at: www.ssi.gouv.fr.
33. Decree from the 11th of August 2016 establishing security rules, modalities for the declaration of information systems of vital importance, as well as security incidents relating to the sub-sector for 'Hydrocarbon Provision', 2016, available at: www.legifrance.gouv.fr.
34. *Ibid*.
35. *Ibid*.

The level of detail and precision contained in French regulation is comparable to that of the American NERC-CIPs, as well as the different Executive Orders and Presidential Policy Directives. Indeed, when it comes to developing rigorous cybersecurity norms, French legislation is not lagging behind its American counterpart in any noticeable way. For instance, the ANSSI possesses coercive powers comparable to those of the NERC in order to verify the implementation of cybersecurity norms. This includes the possibility for the ANSSI to impose fines that can reach up to €150,000 for individuals and €750,000 for legal persons. Moreover, the ANSSI also organizes technical controls and regular inspections of French OVIs, and has put in place a system of alerts with the obligation for OVIs to notify the ANSSI without delay of any incident related to cybersecurity. Nevertheless, one of the main differences between France and the United States is that the latter possesses a specialized agency for the energy sector, since NERC's mandate focuses on the 'bulk power system'.[36] By contrast, the ANSSI's mission is much broader because it must ensure the security of all information systems, including for the energy sector.[37]

Thus, the advantages of the American model are that the NERC can concentrate specifically on cybersecurity for energy firms and other actors, and thus potentially provide a more tailored and rapid response compared to the ANSSI, whose general mandate prevents any such specialization. Indeed, energy is a sector with a certain number of particularities, which deserve their own specific regulations and institutions in order to manage cyberattacks more effectively. Consequently, France could draw inspiration from the NERC in order to put in place a new structure that would be affiliated to the ANSSI; this includes the possibility of creating a sub-direction within it, which would specialize in the energy sector. The objective would be to develop a direct and regular contact with all electric utilities, firms and other actors in the energy sector in France, based on the American NERC model. This would make it possible to establish a more thorough and detailed system of information exchange, helping to develop cybersecurity measures that are better adapted to the specificities of the energy sector. Likewise, it may also be helpful to put in place a specialized cyber alert system for French electric utilities based on the NERC Alerts in the US, which would allow for a more rapid and synchronized response from energy firms and other actors in the event of a cyberattack.

36. As mentioned above, another difference between France and the US is that the ANSSI, like ENISA at the European level, is a public institution, whereas the NERC is a private organization under the supervision of a federal agency (the FERC).
37. The ANSSI has a manager responsible for sectorial coordination with the energy and nuclear sectors, but no specialized agency like the NERC.

Comparative perspectives: what the United States can learn from Europe

The protection of the network for electricity distribution

An important difference between the EU and the US concerns the protection of the network for electricity distribution. Although it exists under different configurations, the electricity network traditionally begins with the generation of electricity, followed by transmission, and finishes with distribution at the level of the consumer. In the United States, even the latest versions 5 and 6 of the NERC-CIPs, as well as the different Executive Orders and Presidential Policy Directives on this subject, do not protect the network at the level of electricity distribution; this responsibility has been left to individual US states. The latter have been highly reluctant to accept any form of federal regulation on this matter and have successfully resisted NERC's efforts to establish security norms at the level of distribution. In spite of this, however, few US states have taken up their responsibilities in this area. In 2015, for example, only five US states had passed laws to reinforce cybersecurity for electricity distribution, with California leading the way.[38] This situation represents a major weakness in the security of the American electricity network. Indeed, millions of smart meters are going to be installed in the US in the years to come, all of which form part of the distribution section of the electricity network, and are thus not covered by the NERC-CIPs. In addition to exposing consumers to privacy and personal data breaches, these new smart meters also present an opening to the physical and material damage that malicious software could potentially cause. Thus, it would be beneficial to update American regulations, and the US could potentially draw inspiration from European legislation in this area. For example, the NIS Directive is explicit on the fact that the distribution section of the electricity network is included in its definition of 'operators of essential services' and must therefore be covered by the cybersecurity

38. See: Shea D., "State Efforts to Protect the Electric Grid", *National Conference of State Legislatures*, 2016, available at: www.ncsl.org.

policies that the law establishes.[39] This incorporates a framework for the prevention and management of cyberthreats, which is to be administered by CSIRTs, whose mission is to protect all sections of the network, including electricity distribution.

Cybersecurity for renewable energies and low carbon technologies

Cybersecurity for renewable energies and low carbon technologies represents another subject where the United States could learn from the EU. Renewable energy infrastructures are particularly vulnerable to cyberattacks, in part due to the intermittence of solar or wind power, which requires advanced technologies for long distance control, insertion into networks and also, increasingly, for storage. In 2013, a group of hackers known as *Dragonfly* succeeded in exploiting these vulnerabilities by introducing malicious software into several renewable energy companies in the US and Europe (including in Germany), which infected a number of industrial control systems. Although these viruses had been conceived mainly for industrial espionage, subsequent investigations have demonstrated that they also had the capacity to take physical control of the infrastructure, with the potential to cause major damage.[40]

The *Clean Power Plan* signed by former President Barack Obama in 2015 did not include specific measures for cybersecurity; moreover, Donald Trump signed an executive order on 29 March 2017 to abrogate it. Indeed, the climate skepticism of the Republican Party will in all likelihood prevent any federal legislation on this issue as long as it remains in power. Nevertheless, even in US states that have announced their intention to continue implementing climate policies, including California and states on the East Coast, cybersecurity is only rarely integrated into renewable energies. This is linked in many ways to the reluctance of US firms to invest in this area. Indeed, an excess of security has been perceived by a number of constructors as representing a risk to innovation and infrastructure efficiency, which could jeopardize profits and their margin for maneuver. According to one of the experts interviewed for this paper, many car manufacturers in the US worry that cybersecurity procedures such as the regular re-initialization of passwords could become overly burdensome for users. By contrast, the EU has begun to integrate cybersecurity into its policies for transitioning towards renewable energies. For instance, in the

39. This is underlined in Annex II of the Directive (sub-section 1-a), which mentions “managers of the distribution network” as a type of entity covered in the sub-sector for electricity.
40. Ruhle M. and Trakimavicius L., “Cyberattacks Are the New Challenge for Renewable Energy”, POLITICO, 23 July 2017, available at: www.politico.eu.

'Winter Package' set out by the European Commission in November 2016 entitled 'Proposals on Clean Energy for all Europeans', there are explicit references to cybersecurity issues. The Winter Package outlines precise policies to protect European renewable energy infrastructure from cyberattacks. This includes the obligation for each new low carbon technology to identify potential cyber threats, as well as the creation of technical rules such as a 'network code' on cybersecurity in order to protect renewable energy technologies. These types of measures would be easily transposable to the United States, and those states that wish to continue their renewable energy policies could learn from EU legislation in this area.

The protection of privacy and personal data

Cybersecurity relates not only to malicious software that can cause material and physical damage; it also includes the theft and hacking of personal data for lucrative purposes, often in relation to commercial spying. The digitization of energy systems is increasingly exposing consumers to the theft of their personal data, which violates fundamental rights linked to privacy protection. This threat will undoubtedly increase in the years to come due to the large-scale deployment of millions of smart meters in the EU and the US. Although one of the purposes of smart meters is to rationalize energy consumption by reducing wastage, they also expose consumers to a higher risk of personal data theft.[41] It is important to distinguish between data protection, which focuses on preventing the excessive collection of personal data from the outset, and data security, which relates to how such data is managed once it has been collected. The US federal legislative system has not been able to pass any laws on data protection, in large part due to powerful lobbies that have successfully blocked the efforts of Congress. As a result, this responsibility has been left to individual states; but, besides California and a small number of other states, most have not passed any meaningful legislation in this area. When it comes to data security, certain laws have been approved by the federal Congress, but they have tended to favor firms and corporations over individuals, which is the case for example with the Cybersecurity Information Sharing Act (CISA), ratified in 2015.[42]

41. Due to their dependence on the Internet, each smart meter represents a potential entry point for malicious software, which then risks spreading to the entire electricity network.

42. The objective of CISA is to ensure the security of data from firms that accept to exchange information with the federal government through the creation of 'safe harbors' that protect against any judicial proceedings. Since consumers are the ones who are most likely to launch such legal

By contrast, the EU has successfully implemented some of the most advanced legislation in the world regarding both data protection and data security. Adopted in 2016,[43] the General Data Protection Regulation (GDPR) contains a number of effective measures to reinforce the rights of individuals. This includes an explicit reference to the right to be forgotten in the situation where personal data has been made public on the Internet, as well as direct access to information concerning the manner in which personal data has been treated. Likewise, the GDPR provides for a right to portability in order to facilitate the transmission of data between operators, a reinforcement of the explicit notion of consent for the treatment of data, as well as an increase in the powers of competent regulatory authorities to impose sanctions and fines. Furthermore, the GDPR also obliges relevant actors to conduct regular analyses concerning the impact of their activities on the protection of consumers' personal data. As a result, the European Commission has put in place a 'data protection impact assessment template for smart grid and smart metering systems', in cooperation with the private sector.[44] Following the launch of the first phase in 2014, this framework has allowed firms to plan their investments in smart networks by anticipating from the outset potential risks relating to data protection.

There is no equivalent at the national level in the United States. Because of the pressure from lobbying groups that have blocked the actions of Congress in this area, it will probably be difficult to put in place any type of federal legislation similar to the EU's GDPR, at least in the near future. Consequently, US states will have to act on this issue, since lobbying obstruction is less problematic at the local level. States that have already implemented certain policies in this area, as well as those that would like to do so, could rely on European legislation as a model for the development of privacy protection for consumers. What is more, since July 12th 2016, an EU-US Privacy Shield has been established in order to reinforce the protection of personal data in transatlantic commercial exchanges. This framework contains a series of measures so that firms on both sides of the Atlantic respect European legislation with respect to personal data protection during commercial transactions. Although US firms do not have an obligation to

proceedings against firms to ensure the protection of their personal data, the end result is to exacerbate the violation of privacy for individuals.

43. The GDPR replaced the 1995 Directive on data protection in order to provide consumers with more control and a better access to their personal data, as well as dispositions to protect European citizens' data all around the world, even outside the EU. See: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, available at: http://eur-lex.europa.eu.

44. European Commission Recommendation on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, 10 October 2014, available at: http://eur-lex.europa.eu.

join the privacy shield, once they have officially made that choice, they are accountable before American courts.[45] Moreover, European firms have a tendency to prioritize commercial accords with those American firms that are part of the privacy shield. This means that US companies are under pressure to comply with European rules regarding data protection if they want to have access to the EU internal market. Given that the EU represents the first commercial partner of the United States, the privacy shield provides an effective tool so that European norms for personal data protection can spread to American soil, despite the absence of federal legislation in this area. This has a direct impact on the energy sector due to the accelerating digitization of the electricity network, which is leading to an increase in the number of transatlantic commercial exchanges regarding the installation of smart meters.

What the United States could learn from the French model

France is relatively advanced compared to the United States in terms of the protection of privacy and personal data. Indeed, France possesses its own national institutions in this area, such as the National Commission on Informatics and Liberty (*Commission nationale de l'informatique et des libertés*, CNIL), mentioned above. Created in 1978, this institution is charged with ensuring that information technologies are at the service of citizens; the commission has a mandate to defend human rights and human identity, as well as to protect privacy, and individual and public liberties. This mandate is articulated in the January 6, 1978 law, modified in August 2004, relating to informatics, data files and liberties (*Loi relative à l'informatique, aux fichiers et aux libertés*). Although there are other similar institutions in Europe, the CNIL is considered to be one of the most active and, more importantly, there is no equivalent in the United States. Indeed, the only American federal institution in this area is the Privacy Office of the U.S. Department of Homeland Security, created in 2002, which is supposed to have a mandate to act on personal data protection. Nevertheless, the problem is that this Privacy Office is subordinate to the Department of Homeland Security, whose priority is above all to ensure national security. Moreover, the absence of any federal legislation for data protection, and its inadequacy regarding data security, considerably reduce the Privacy Office's margin for maneuver.

45. US Department of Commerce, *Overview of the EU-US Privacy Shield*, 12 July 2016, available at: www.commerce.gov.

By contrast, the CNIL constitutes an administrative authority that is independent from any public or private entity, and whose neutrality is guaranteed by its composition and organization. The President of the CNIL is freely elected by its members and does not receive instructions from any public or private authority; no cabinet minister, business leader or CEO has the power to oppose his or her actions.[46] Likewise, the CNIL can also rely on very extensive French and EU legislation regarding privacy protection, which provides it with a solid basis to carry out its mission. As a result, the CNIL possesses a much broader mandate compared to the US Privacy Office, which includes informing, protecting, accompanying and advising both public and private entities, as well as punishing when necessary any violation of individual freedoms. The CNIL is also charged with anticipating risks in relation to new digital technologies and possesses its own laboratory to test innovative products and software.[47] Even though the United States is blocked at the federal level due to the pressure exercised by powerful lobbying groups, the state and local levels are less constrained by this type of impediment. American states that have already implemented certain regulations in this area, as well as those that wish to do so, could learn from the CNIL when it comes to the protection of privacy and personal data.

46. The CNIL in France – *How it functions*, available at: www.cnil.fr.
47. The CNIL in France – *Its missions*, available at: www.cnil.fr.

Reinforcing transatlantic cooperation to develop common standards

The EU and the United States have very different approaches regarding cybersecurity for energy infrastructure. On the one hand, the American approach has been to focus on a 'security in depth' strategy involving strict and detailed regulations in precise sectors, which are implemented by institutions with coercive powers. On the other hand, the EU's strategy is more flexible and exhaustive, as it prioritizes the protection of a wide range of different sectors such as electricity distribution, renewable energies and personal data. Thus, it appears that the European and American approaches are potentially complementary, with a strong possibility for greater collaboration. Consequently, it would be advantageous to enhance transatlantic cooperation regarding cybersecurity, allowing the US and the EU to learn from one another by reinforcing dialogue and information sharing. Following Donald Trump's election, transatlantic relations have entered into a period of uncertainty.[48] Nevertheless, President Trump has demonstrated a notable interest for cybersecurity issues by reinforcing the measures taken by his predecessor in this area.

As a result, in spite of current disagreements on a number of issues, cybersecurity represents a domain where there exists a real opportunity to strengthen transatlantic cooperation in the years to come. This would be beneficial for both sides, given the complementarity of their respective approaches. Moreover, a reinforced transatlantic partnership could contribute to the development of common international cybersecurity standards that would be amongst the most advanced in the world; these could in turn serve as models for other countries to follow. Due to the globalization of digital technologies, a cyberattack even in an apparently remote country can spread and affect networks in Europe and the US. This is precisely what happened with the *NotPetya* virus, which spread to many Western firms with commercial relations in Ukraine, including through subsidiaries and sub-contractors spread across many countries. Consequently, a more effective transatlantic cooperation allowing for the

48. Gomart T. (ed.), "Trump, un an après. Un monde à l'état de nature?", *Études de l'Ifri*, Ifri, November 2017, available at: www.ifri.org.

development of rigorous international norms could contribute to reducing the risks of propagation.

Bilateral cooperation between governments

Bilateral cooperation between governments represents the most direct and one of the most effective ways to develop common transatlantic standards. Since 1991, an annual EU-US summit has been organized in order to reinforce cooperation in a number of different areas. Over the last few years, issues relating to the energy sector and cybersecurity have become more important, and several high-level platforms have been created specifically in these areas. This includes the EU-US Energy Council since 2009, the EU-US Cyber Dialogue since 2014, the EU-US Working Group on Cybersecurity and Cybercrime since 2010, as well as the Information Society Dialogue since 2002. Nevertheless, while these four platforms allow the EU and the US to collaborate on concrete policy issues, none of them focuses specifically on cybersecurity in the energy sector, even though they work on related topics. As a result, one option would be to create a new transatlantic platform dedicated specifically to this subject, which could take the form of an annual summit at the Ministerial level in order to encourage the development of common norms. Another, more easily achievable solution would be to create new working groups within the four existing platforms, which could focus specifically on cybersecurity in the energy sector. The objective would be to encourage these different working groups to collaborate by establishing an ongoing dialogue and regular information sharing.

For example, during the 7th EU-US Energy Council in May 2016, both partners issued a common declaration indicating their willingness to reinforce cooperation on new digital technologies. This includes smart meters, an area where cybersecurity plays an essential role.[49] Similarly, during the third meeting of the EU-US Cyber Dialogue in December 2016, both partners expressed their desire to strengthen collaboration regarding cybersecurity in critical infrastructure,[50] with strong potential to include the energy sector. Moreover, the EU-US Working Group on Cybersecurity and Cybercrime established on a regular basis a synchronized 'Cyber Awareness

49. Moreover, there is already an existing partnership between the American FERC and the European Commission's DG for Energy within the framework of the EU-US Energy Council. Although the latter focuses on the regulation of energy markets, its mandate could be broadened to cover cybersecurity issues, which have a direct impact on energy markets. See: 7th US-EU Energy Council, *Joint Statement,* European External Action Service, May 2016, available at: https://eeas.europa.eu.

50. *Third meeting of the EU-US Cyber Dialogue*, European External Action Service, December 2016, available at: https://eeas.europa.eu.

Month' in Europe and the US. Since the latter has focused on industrial control systems, there is a possibility to integrate issues relating to the energy sector. Finally, during the fourteenth gathering of the Information Society Dialogue (ISD) in June 2016, the EU and the US confirmed their desire to work together on privacy protection in the development of new digital technologies.[51] Consequently, the impact of smart meters on the protection of personal data in the electricity network should play a larger role in future ISD summits. Due to Donald Trump's foreign policy orientation, however, there are currently doubts regarding whether or not these four platforms for transatlantic cooperation will be maintained. Thus, it is essential that the EU do everything it can to convince the Trump administration of the major benefits that these platforms can provide in terms of dialogue and information sharing. On both sides of the Atlantic, governments are confronted with the same growing challenges, which can only be overcome through reinforced cooperation.

Transatlantic collaboration in a multilateral framework

Bilateral transatlantic cooperation needs to be reinforced through a multilateral institutional framework. Indeed, the objective would be for transatlantic cybersecurity standards to be shared so that they could become rigorous international norms. There are several multilateral institutions where the EU and the US collaborate with other countries on cybersecurity issues, including NATO.[52] The organization possesses more than a decade of experience in this area, with the 2002 Prague summit establishing cybersecurity on the Alliance's political agenda for the first time. In July 2016, the Allies recognized cyberspace as constituting a high priority issue and a sector of operation where NATO must develop the means to defend itself as effectively as on land, at sea or in the air. Since 2010, NATO has also organized an annual large-scale cybersecurity exercise ('Locked Shield Cyber Exercise') that involves many countries and simulates a massive cyberattack on computer networks. The 2017 version of the Locked Shield Cyber Exercise simulated a cyberattack on the electricity network, which is encouraging for cybersecurity in the energy sector in the years to come.[53] It is essential that this type of exercise be repeated on a regular basis, since a significant cyberattack on the energy sector could have major consequences

51. *Joint Statement of the 14th EU-US Information Society Dialogue*, European Commission – Digital Single Market, June 2016, available at: https://ec.europa.eu.
52. Despite criticism during the Presidential campaign, Trump has since then reaffirmed his support for NATO, underlining the possibility for transatlantic cooperation within this institution.
53. Currently, NATO's priority regarding cybersecurity is to protect its own networks, especially its military infrastructure. See: NATO, *Cyber defense*, August 2017, available at: www.nato.int.

on NATO's military potential. In addition, during the 2016 Warsaw summit, the Allies reaffirmed that improving cybersecurity for critical infrastructure should be a top priority, which includes by extension the energy sector. What is more, NATO and the EU signed a technical cooperation agreement regarding cyberdefense in February 2016, which includes information sharing and common exercises. This arrangement could provide a springboard to reinforce NATO capabilities in relation to cybersecurity for energy infrastructure. For example, it would be beneficial to systematically include the electricity network during Locked Shield Cyber Exercises, and perhaps also integrate nuclear power plants during simulations due to their strategic importance.

The G7 is another essential multilateral institution where Europe and the US collaborate with other world powers, including on issues relating to cybersecurity and the energy sector. For example, the G7 summit held in Japan in May 2016 led to a number of major advances in these areas. Heads of state and government agreed on a roadmap to develop common international standards on cybersecurity, including for critical infrastructure (the G7 Principles and Actions on Cyber)[54]. They also created a new permanent working group specialized in cybersecurity issues (the Ise-Shima Cyber Group), which will need to work in collaboration with the other existing working group (the G7 Cyber Expert Group). The 2016 summit also organized a meeting between Energy Ministers from member states, who agreed on a number of measures, including for cybersecurity (the Initiative on Energy Security for Global Growth)[55]. For example, international cybersecurity standards were formulated for the gas sector and the electricity network. These measures were confirmed during the 2017 G7 summit held in Italy, in part thanks to the work of the Ise-Shima Cyber Group specialized in cybersecurity, as well as the Energy Ministerial meeting in Rome.

Nevertheless, one of the main weaknesses of the G7 is that common declarations are general in nature and do not set out proposed policies in sufficient detail, which means that international standards risk becoming mere declarations of intention. Moreover, responsibilities between the different working groups and Ministerial meetings have not been clearly delineated,[56] which occasionally results in confusion due to competence

54. *G7 Principles and Actions on Cyber,* May 2016, available at: www.mofa.go.jp.
55. G7 Energy Ministerial Meeting, *Kitakyushu Initiative on Energy Security for Global Growth*, May 2016, available at: www.g8.utoronto.ca.
56. The last few G7 summits also brought together Ministers working on issues relating to information and communication technologies (ICT), allowing for the development of a strategy with common international standards (G7 ICT Strategy), which includes privacy protection in the development of new digital technologies.

overlap. Finally, the work of the G7 regarding cybersecurity has focused above all on the financial system, with the elaboration of a common strategy during the 2016 summit[57], which was reinforced during the 2017 summit.[58] Although cybersecurity for energy infrastructure is mentioned during G7 Energy Ministerial meetings, it is not currently a priority issue. Thus, it is essential for the G7 to assign a more important role to this subject, which could take the form of a new specialized working group that would collaborate with Energy Ministerial meetings. This would help to clarify competence allocation between the different working groups and bring more precision during common declarations.

Transatlantic partnerships between firms and industrial groups

In Europe and in the United States, private companies and industrial groups play an essential role in the development of standards and best practices for cybersecurity, in collaboration with the public sector. For example, a number of European countries have developed official public-private partnerships to support cybersecurity, and different national industries have set up cybersecurity councils made up of business representatives.[59] At the level of the EU, a Contractual Public Private Partnership (cPPP) was established in July 2016 that includes the European Commission and the European Cyber Security Organization (the latter brings together public and private actors that work in partnership with the Commission under the framework of the cPPP).[60] The objective of this partnership is to reinforce cooperation between the public and private sectors in order to strengthen cyberdefense mechanisms for critical infrastructure, including the energy sector.[61] Furthermore, the Cybersecurity Package proposed by the European Commission in September 2017 seeks to establish an EU certification system

57. *G7 Fundamental Elements of Cybersecurity for the Financial Sector*, May 2016, available at: www.treasury.gov.
58. *G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector*, October 2017, available at: www.g8.utoronto.ca.
59. This includes Germany, Austria, Spain and the Netherlands, for example. See: BSA / The Software Alliance, *EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace*, January 2015.
60. The European Cyber Security Organization (ECSO) is a self-financed, nonprofit organization governed by Belgian law that was established in June 2016. It brings together all relevant actors from both the public and private sectors that participate in the cPPP, together with the European Commission. See: ECSO, *Mission & Objectives*, available at: https://ecs-org.eu.
61. The EU intends to support the cPPP with up to 450 million euros, with an anticipated additional investment of one billion euros from the private sector. See: European Commission, *Commission Signs Agreement with Industry on Cybersecurity and Steps up Efforts to Tackle Cyber-Threats,* 5 July 2017, available at: http://europa.eu.

under the aegis of ENISA.[62] The objective is to facilitate the development of a European internal market for cybersecurity and reinforce public-private sector cooperation; policies in this area were outlined in more detail during the Digital Summit that took place in Tallinn in September 2017.

In the United States, the Cybersecurity Risk Information Sharing Program ('CRISP') represents one of the main partnerships between the energy industry, the Department of Energy (DOE), as well as the DOE Office of Electricity Delivery and Energy Reliability (DOE-OE). CRISP allows the different actors to exchange information about cybersecurity on a regular basis and in a structured manner. This partnership has worked well, as a majority of businesses from the energy sector have agreed to participate, representing 75% of American consumers. Furthermore, since 1998, industrial operators collaborate with the US federal government to identify cyberthreats and protection standards through institutions called Information Sharing and Analysis Centers (ISACs). In 2015, former President Obama created the Information Sharing Analysis Organizations (ISAOs) in order to encourage firms that have not been able to join the ISACs to still have the possibility of collaborating with the federal government, including through information sharing. There is also a specialized ISAC for the electricity sector (E-ISAC), which serves as the principal intermediary between the Department of Energy and electric utilities for coordination and the exchange of technical information.

Nevertheless, despite recent progress on these issues, most of the experts interviewed for this paper agree that information exchange between the public and private sectors remains insufficient both in Europe and the United States. This is mainly due to the fact that firms are often reluctant to notify government agencies if they are hit by a cyberattack because of the damage this could cause to their reputation. Consequently, supporting transatlantic cooperation in this area could contribute to reinforcing public-private partnerships on both sides of the Atlantic. The objective would be for European and American public-private partnerships to collaborate in order to develop common norms. Although there are several existing platforms that encourage transatlantic cooperation between firms on related subjects, none of them specializes in cybersecurity for the energy sector. As a result, one solution would be to create a new transatlantic framework dedicated specifically to cybersecurity for energy firms, which would bring together the different public-private partnerships through regular meetings and information sharing. Another possibility would be for these partnerships to join existing structures that work on transatlantic commercial exchanges. For example, the Transatlantic Business Council has been organizing a

62. European Commission, *New Cybersecurity Package*, September 2017.

Digital Economy Workshop ('DEW') on a regular basis since 2002. It represents one of the main events of the Information Society Dialogue, and focuses amongst other things on the development of security standards for new ICTs. Furthermore, the EU-US Innovation and Investment in the Digital Economy Dialogue (IIDED), whose first meeting took place in Boston in March 2016, covered matters relating to new digital technologies. In both cases, the DEW and the IIDED work on issues that are directly related to European and American public-private cybersecurity partnerships in the energy sector. Therefore, it would be beneficial if the latter would participate on a regular basis in order to encourage the development of common transatlantic standards.

Conclusion

The United States and the European Union have different approaches regarding cybersecurity in the energy sector. The American strategy has been to favor 'security in depth' with strict and detailed regulations in specific sectors, implemented by federal institutions with coercive powers. On the contrary, the EU has adopted a more flexible and exhaustive strategy, covering a wide range of different sectors and leaving an important margin of maneuver to member states for the implementation of norms. Nevertheless, these approaches are complementary in that they represent two sides of the same coin. Indeed, the strengths of the American system can serve as a model to improve certain weaknesses in the European approach, and vice versa, since the EU also possesses a certain number of assets that the US could learn from. On the one hand, the US is ahead regarding the development of precise and detailed norms for cybersecurity in the electricity sector, as well as for the implementation of these norms, where the EU could draw inspiration from the American model. On the other hand, the US could learn from the EU on issues such as the protection of privacy and personal data, cybersecurity for low carbon technologies, as well as the protection of electricity distribution. Moreover, California and France are examples of a US state and an EU country that present a number of interesting specificities in this area.

As a result, there is a real opportunity to develop a stronger transatlantic partnership on cybersecurity, allowing the EU and the US to learn from each other's frameworks. This would need to take place on several different levels, including reinforced bilateral cooperation between governments, within multilateral structures such as NATO or the G7, and also through public-private partnerships. The objective would be to establish common transatlantic standards on cybersecurity, which could then become rigorous international norms. Due to the globalization of digital technologies, a cyberattack even in a remote country risks spreading to the entire network, which was highlighted by the recent events in Ukraine. Therefore, if the EU and the US succeed in strengthening international norms on cybersecurity, this could help to reduce the risks of propagation. As the digitization of critical infrastructure accelerates, the subject of cybersecurity in the energy sector will be of seminal importance in the years to come. This is partly due to the rise of cyber espionage and cybercriminality, where malicious software is increasingly used to hack data

for commercial purposes. Moreover, due to the currently volatile context of international relations, the growth in cyberattacks has accompanied the rise in tensions between the great powers. It is for these reasons that the EU and the US have a particular responsibility, since their collaboration on cybersecurity issues is essential. Despite disagreements with the EU on a number of subjects, President Trump has demonstrated a notable interest for cybersecurity, which represents an area where there is a real opportunity to enhance transatlantic cooperation in the years to come.

References

ANSSI, *Maîtriser la SSI pour les systèmes industriels*, 2012.

ANSSI, "Stratégie de la France : défense et sécurité des systèmes d'information", 2011.

ANSSI, "Stratégie nationale pour la sécurité du numérique", 2015.

BSA/The Software Alliance, *EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace*, January 2015.

California Legislative Information, "AB-1274 Privacy: Customer Electrical or Natural Gas Usage Data", October 2013.

Cruciani M., "The Landscape of Renewable Energy Sources in Europe in 2030", *Études de l'Ifri*, Ifri, June 2017.

Desarnaud G., "Cyber Attacks and Energy Infrastructures: Anticipating Risks", *Études de l'Ifri*, Ifri, January 2017.

Ebinger C. and Massy K., "Software and Hard Targets: Enhancing Smart Grid Cyber Security in the Age of Information Warfare", *Energy Security Initiative at Brookings*, 2011.

EECSP, *Cyber Security in the Energy Sector: Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector*, 2017.

ENISA, *Cybersecurity cooperation: defending the digital frontline*, 2013.

ENISA, *Cyber Europe 2016: After Action Report*, June 2017.

ENISA, *Good Practice Guide for Incident Management*, 2010.

ENISA, *Multi-Annual Staff Policy Plan 2016-2018*, October 2015.

ENISA, *Report on Cybersecurity Information Sharing in the Energy Sector*, 2016.

ENISA, *Statement of Estimates 2017* (Budget 2017), 2017.

European Commission, *Commission Signs Agreement with Industry on Cybersecurity and Steps up Efforts to Tackle Cyber-Threats*, 5 July 2017.

European Commission, *New Cybersecurity Package*, September 2017.

European Parliament, Directorate General for Internal Policies, *Cyber Security Strategy for the Energy Sector*, Study for the Industry, Research and Energy Committee, October 2016.

EU-US Cyber Dialogue - Third meeting, December 2016, https://eeas.europa.eu.

EU-US Energy Council, *Joint Statement*, 2016.

EU-US 14th Information Society Dialogue, *Joint Statement*, 2016.

Fallon R. and Lazaroff M., *NERC Increasing Penalties for Fundamentally Failing to Comply with Cyber Standards*, Cozen O'Connor, November 2016.

Global Cybersecurity Summit 2017, which took place in Kiev, Ukraine from 14 to 15 June 2017, https://gcs17.com.

Gomart T. (ed.), "Trump, un an après. Un monde à l'état de nature?", *Études de l'Ifri*, Ifri, November 2017.

Guiton A., "Enquête : les cobayes de la cyberguerre", *Libération*, 28 July 2017.

G7 Principles and Actions on Cyber, 2016.

G7 Fundamental Elements of Cybersecurity for the Financial Sector, 2016.

G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector, 2017.

G7 Kitakyushu Initiative on Energy Security for Global Growth, 2016.

IAEA, "Computer Security at Nuclear Facilities", *Security Series No. 17: Technical Guidance Reference Manual*, 2011.

Lindsay J. R., "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack", *Journal of Cybersecurity*, Volume 1, Issue 1, 1 September 2015.

NATO, *Cyber defence*, August 2017, www.nato.int.

NERC 2017 Business Plan and Budget Final Draft, Finance and Audit Committee Meeting, August 2016.

O'Keefe E. and Nakashima E., "Cybersecurity Bill Fails in Senate", *The Washington Post*, 2 August 2012.

Ruhle M. and Trakimavicius L., "Cyberattacks Are the New Challenge for Renewable Energy", POLITICO, 23 July 2017.

SANS and E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*, 2016.

Shea D., "State Efforts to Protect the Electric Grid", *National Conference of State Legislatures*, 2016.

US Chamber of Commerce, *Transatlantic Cybersecurity: Forging a United Response to Universal Threats*, 2017.

US Department of Commerce, *Overview of the EU-US Privacy Shield*, 12 July 2016.

World Energy Council, "The Road to Resilience: Managing Cyber Risks", *World Energy Perspectives*, 2016.

ifri
institut français
des relations
internationales