WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Shaping the Future of Cybersecurity and Digital Trust

Cyber Resilience in the Electricity Industry:

Analysis and Recommendations on Regulatory Practices for the Public and Private Sectors

In collaboration with Accenture and the Electricity Industry Community

July 2020

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

Contents

Executive summary

The objective of this report is to provide recommendations to both policy-makers and companies to improve cybersecurity resilience in the electricity sector.[1] Cyber resilience, which looks beyond regulatory compliance and cybersecurity, addresses the capacity of utilities to prepare for, respond to and recover from cyberattacks. It emphasizes a proactive posture that mitigates risk, limits the impact of attacks and facilitates continuity of operations for the electricity sector in the face of challenging conditions.[2]

A variety of threat actors continually target power utilities, seeking to profit financially or otherwise cause harm using attack vectors such as ransomware or by disrupting the availability of critical functions.

According to the World Economic Forum *Global Risks Report 2020*, cyberspace has become an extension of the military domain, and this has triggered a technological arms race.[3] Cyberattacks on critical infrastructure were ranked the fifth top risk in 2020 for multiple sectors, including energy.[4]

Utilities must adapt to the pace of change in the digital threat landscape, so as to prevent exposure to higher-volume, larger-scale and more sophisticated attacks. At the same time, regulators are challenged to keep regulations current. Certainly, regulations are important to establish a common baseline of cybersecurity practices for essential services. In addition, companies often need such regulations to justify investments for the implementation of cybersecurity controls. Yet the challenge lies in moving beyond regulatory compliance to an approach focused on cybersecurity risk as a whole.

Cyberattacks on critical infrastructure, particularly in the electricity sector, could generate devastating cascading effects, resulting in loss of life, economic costs and industrial disruption, among other severe consequences. Moreover, the electric utilities market is evolving, with increasing digitalization and changes to the attack surface, requiring the electricity sector and its regulators to respond. With the goals of lowering cost, decentralization, decarbonization and better returns on investment, this transformation is also accelerating the convergence of information technology (IT) and operational technology (OT), adding increased connectivity to industrial control systems (ICSs) for critical infrastructure, compounded with the growth of the industrial internet of things (IIoT) and accompanying risks (see Appendix A).

The World Economic Forum's Systems of Cyber Resilience: Electricity project is a public-private collaboration initiative with the objective of enhancing cyber resilience across the electricity ecosystem through thought leadership and concerted action.[5]

This analysis was centred on North America and Europe as a starting point to encourage dialogue with policy-makers and utilities in these two large regions and illustrate the effects of the current regulatory practices and opportunities to bridge the gaps between regulations and cybersecurity risks in the electricity sector. Many, if not most, insights and recommendations may apply to other geographies.

The structure of this report covers: 1) threat landscape and emerging risks; 2) regulatory landscape and analysis of EU-US regulations; 3) international best practice frameworks and standards; 4) certification; and 5) regulatory practices.

Gaps identified by the detailed analysis outlined in this report provide opportunities for improvement of cyber resilience for both regulators and utilities. Initial findings from these contributions and analysis recommend the following collective actions:

- Development of principle-based global cybersecurity regulatory guidance, enabling utilities to align their cybersecurity practices across regions, enhancing flexibility
- A common product certification approach, with limited and specific use cases, to assist utilities in securing their supply chains
- Enhanced collaboration across government, industry, academia and supply chains, leading to more flexible, effective and targeted regulatory and information-sharing practices

1.0 State of play

In recent years, both national and international headlines have highlighted the impact of cyberattacks on the electricity sector.

FIGURE 1. EXAMPLES OF CYBER INCIDENTS AND EVENTS AFFECTING THE ENERGY SECTOR (2010–2020)

US

Multistage nation state spear-phishing campaign with staged malware, gained remote access and collected critical information (2018)

Snipers fired on Metcalf electrical substation, disabled 17 giant transformers (2013)

Counterfeit Yokogawa instruments for control systems discovered (2019)

Brute-force attack used to hack passwords on utility network (2014)

Firewall firmware vulnerabilities used to cause denial of service attacks, affecting utility control centre (2019)

Large utility fined $10 million for multiple regulatory compliance violations (2019)

Ukraine

Black Energy attack on Ukraine energy companies left 225,000 citizens without power (2015)

Crash Override/Industroyer attack affected substations, and almost a quarter of the Ukraine power grid (2016)

EU

Phishing emails sent to senior engineers working for Ireland's distribution system operator attempted to affect power grid (2017)

Virtual wire tapping of unencrypted traffic from transmission operator in UK passing through routers in Northern Ireland and Wales (2017)

Organization serving multiple utilities hit with cyberattack, causing project delays (2020)

Ransomware attack strikes large utility, supposedly stealing 10 TB of sensitive data, with a threat to expose it if not paid a ransom (2020)

Iran

Stuxnet affects centrifuge control systems, causing malfunction, destruction and significant political consequences (2010)

Saudi Arabia

Shamoon virus shut down 30,000 control systems, erasing data on hard drives and causing severe damage (2012); follow-on attack (2016/2017)

Multinational

VPNFilter infects more than 500,000 routers worldwide, exfiltrating credentials and rendering network-attached devices useless (2017)

Dragonfly/Energetic Beat gained full control, and collected data using trojan backdoors (2014)

1.1 Emerging risks

Globally, there has been an increased emphasis on automation, decarbonization, decentralization and digitization of energy, along with more significant movement towards cleaner energy technologies and modernization of critical infrastructure. In addition to traditional threats and vulnerabilities affecting critical infrastructure, emerging technologies such as distributed energy resources and electric vehicle (EV) charging stations may increase the attack surface for cyberattacks and generate new attack vectors for cyberthreat actors.

Furthermore, the COVID-19 pandemic is having a dramatic impact on industries and has forced everyone to become heavily reliant on the internet and its digital economy. The large-scale adoption of remote-access technologies to enable work-from-home practices, with a greater reliance on cloud services, enables companies to continue operations and reduce costs in conditions of physical distancing and "stay-at-home" orders from government and/or employers. It is also reshaping the digital landscape and architecture while straining supply-chain resilience and cybersecurity operations with the escalating risk.

1.2 Third-party risk

All electricity industry companies from suppliers to system operators now have global supply chains, emphasizing the need to focus on supply-chain security and resilience.

Cross-border interconnections facilitate additional volumes of renewables and support-system reliability, but also introduce new risks through physical connections with neighbouring grids.

Liberalized electricity markets increasingly depend on the interactions between generation, transmission, distribution and trading functions often provided by separate organizations, each with its own set of organizational and ecosystem risks and risk appetites.

Additionally, customers using new business models (e.g. "as-a-service" and cloud-based) may receive services, maintenance or engineering support from providers spanning multiple areas of the globe.

Utilities and their regulators require additional details to understand how the design, product manufacturing, systems integration and testing may be affected in multiple countries without consistent cybersecurity regulation.

2.0 Legal and regulatory landscape

2.1 Cybersecurity laws and regulations in North America and Europe

The North American Electric Reliability Corporation (NERC) released the initial version of the Critical Infrastructure Protection (CIP) regulatory standards in 2007.[6] Since that time, NERC has continually revised and updated these regulatory criteria based on lessons learned. They are prescriptive standards with steep fines for non-compliance, and they suffer from a level of detail and rigidity that does not always incentivize moving beyond compliance towards a risk-based approach.

In the European Union, the Directive on security of network and information systems (the NIS Directive) was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016.[7] The NIS Directive is Europe-wide cybersecurity legislation that aims to protect critical infrastructure, building on the Council Directive 2008/114/EC of 8 December 2008 while also addressing different objectives.[8]

The NIS Directive will be interpreted and implemented by each member state and enforced on those operators identified as providers of essential services.[9] The legislation states that penalties, to be used in case of non-conformity with minimum standards, should be effective, proportionate and dissuasive. Responsibility for defining minimum standards and enforcing compliance lies with the individual member states rather than the EU.

While the focus of this white paper centres on laws and regulations highlighted in Figure 3, the legislation

and associated guidance shown in Figure 2 demonstrates how countries around the world have evolved their cybersecurity strategies with respect to critical infrastructure (sometimes enlarging the target to connected but non-critical infrastructure).

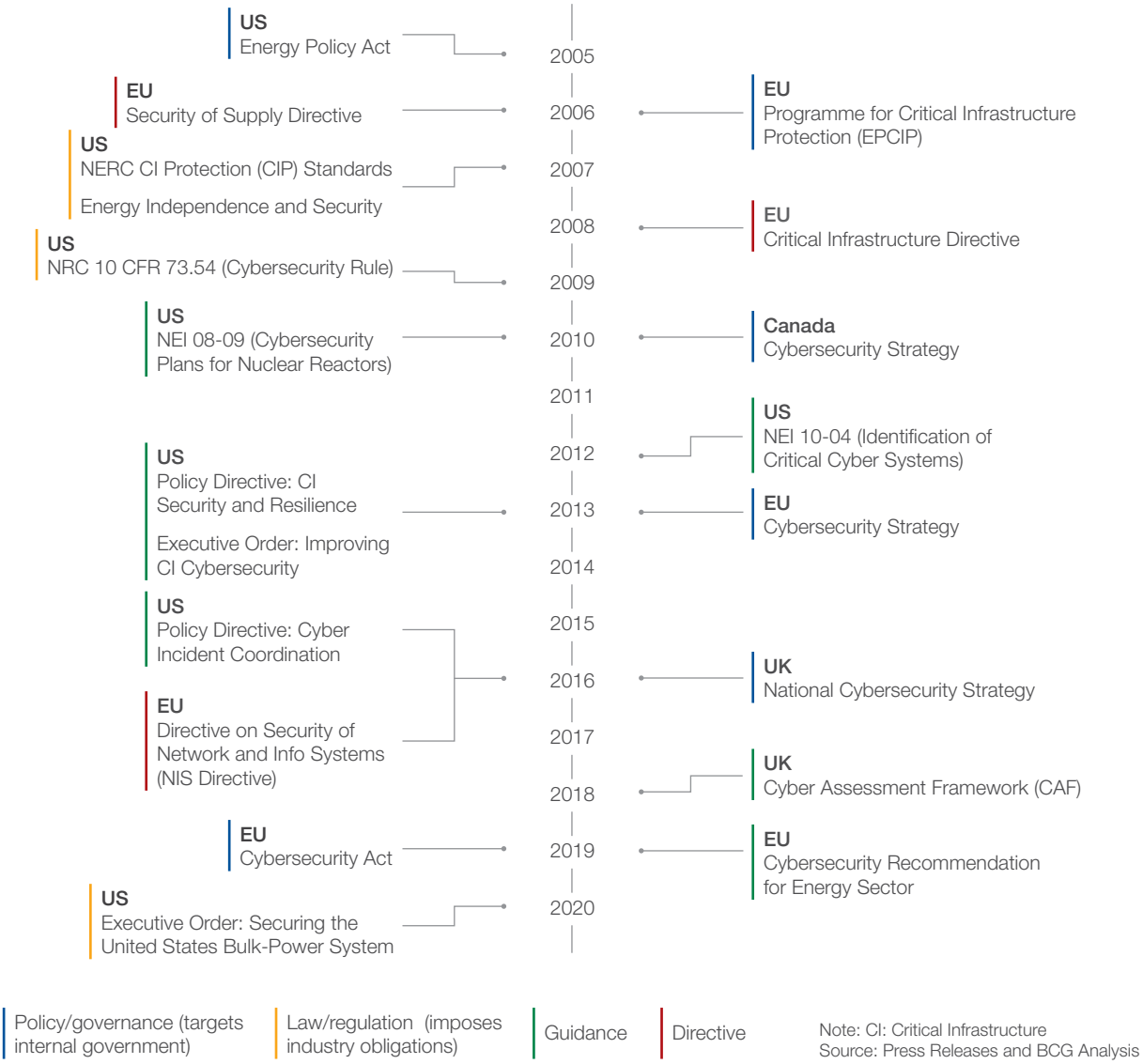
Identifying the similarities and gaps in the various laws, regulations and standards is challenging, given the wide disparity in the construction of the laws and regulations.

Some of these, such as the NERC CIP, impose highly prescriptive and granular mandates on utilities that are backed up by routine audits and sizeable fines. By contrast, European law has until recently focused on high-level frameworks to protect critical infrastructure from cyberattacks.[10]

As threats and technology change, so must laws and regulations. The NERC CIP regulatory criteria and the NIS Directive recognize that the market alone cannot effectively incentivize appropriate cybersecurity practices, particularly in areas of critical infrastructure in which the consequences of a cyberattack can affect critical functions. Besides, the enforcement of non-compliance fines can help ensure that business leaders understand the importance of cybersecurity (see Appendix B).

Lastly, some level of regional alignment is necessary for an industry that crosses national boundaries and depends on multiple actors working in concert to deliver a reliable service to billions of people. The sections that follow will examine those regulatory schemes and related agreements.

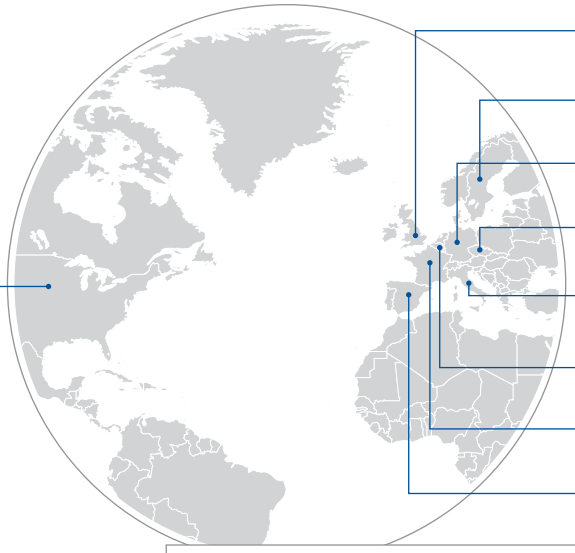
FIGURE 2. NORTH AMERICAN AND EUROPEAN ENERGY CYBERSECURITY POLICIES AND REGULATIONS



2.2 Global analysis of cybersecurity laws and regulations

This analysis focuses on comparing the various laws and regulations in Europe and the United States as far as is feasible. Unlike the broader legislation shown in Figure 2, the laws and regulations referenced in Figure 3 (see Appendix B for more details) are ones that impose requirements, directly or indirectly, on utilities.

FIGURE 3. LAWS AND REGULATIONS REVIEWED



North America
NERC CIP

UK
Ofgem Guidance

Sweden
Security Protection Act

Germany
IT Security Act and IT Security Catalog

Czech Republic
Act No. 181 of 23 July 2014

Italy
DLGS 65/2018 and 133/2019

Belgum
Act of 1 July 2011

France
Decree No. 2018-384/Law 2013/1168

Spain
Res. of 8 Sept. 2015/Law 8/2011

Across EU
Directive on Security of Network and Information Systems (NIS)

EU Cybersecurity Act 2019/881 (not mappable to CSF but relevant for overall context)

New - Electricity Market Regulation (included for context)

New - Risk Preparedness Regulation (included for context)

See Appendix B for a more complete description of the regulations

2.3 Results of legal and regulatory analysis

Detailed analysis generated the following insights and observations:

The NERC CIP requirements imposed on power utilities in North America are the most mature. Still, they suffer from a level of detail and rigidity that does not always incentivize utilities to go beyond compliance with their cybersecurity programmes in order to stay ahead of evolving threats and technological innovations. Fines and regular audits mandated by the requirements also make such adaptation more difficult.[11]

Regulators in countries such as Germany, the Czech Republic, Spain, Italy and France have primarily advocated but not required international standards such as IEC/ISO 27001, IEC 62443 and NIST CSF (National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity) to apply to critical infrastructure/essential service providers. Limited tailoring is applied for power utilities, but these utilities have the ability to select which provisions of the standard to implement. Additionally, the assurance frameworks and processes for verifying compliance are limited, with audits and inspections occurring very infrequently and fines imposed only in the most egregious cases.[12] Often regulators do not have the legal authority to impose a fine. Under the NIS Directive, each country has discretion on when to impose fines and the amount of the fine if the minimum requirements are clearly established.

Many other European countries have very limited or no specific cybersecurity requirements for utilities; what requirements exist are restricted to identifying security points of contact and mandating that a risk assessment be performed – but without reference to the standards to be used or accountability for the results.

The United Kingdom and the nuclear industry offer a balance between the rigid requirements of the NERC CIP and vague criteria applied in much of Europe; for example, the UK's national utility regulator, the Office of Gas and Electricity Markets (Ofgem), instead mandates that the National Cyber Security Centre (NCSC)'s Cyber Assessment Framework (CAF) is referenced. The CAF is based on principles, objectives and outcomes. Operators of essential services, including electricity, are required to manage network and system cyber risks in an appropriate and proportionate manner. They are also mandated to implement effective measures to prevent and minimize the impact of related incidents. Operators may be fined, and in some cases, there may be licensing consequences. Conversely, network companies may choose to submit their cyber-resilience plans for review and approval of strategic funding during price control periods.[13]

Across all cybersecurity laws and regulations in North America and Europe, some gaps have been identified, including:

– **Supply chain** Although most cybersecurity standards reference supply-chain security, interdependencies within the electricity market are different, depending on system operators that may not be able to dictate the behaviour of others by contract. For instance, while the NERC CIP addresses supply-chain risk in its recently adopted CIP-013,[14] there is limited guidance on how to implement a supply-chain security programme that addresses the most relevant risks while not overwhelming the utility.[15] Moreover, targeted efforts such as the recently issued Executive Order on Securing the United States Bulk-Power System[16] and expected guidance from a task force set up by the Executive Order (EO) are only practical and actionable if utilities have robust supply-chain risk management processes that can track the source of all purchases and map them to current assets. It is that detailed and utility-specific guidance that is needed.

– **Cyber resilience** While cybersecurity resilience is mentioned frequently in an aspirational sense in cybersecurity laws, regulations and frameworks, it is often challenging to define what resilience means in a way that is measurable. In most control frameworks, resilience discussions are reserved for mitigation of network denial of service risks. Consequently, there should be more focus on the capacity to maintain integrity in the face of compromised data, component failures or loss of view, and results on manual operations as an aspect of resilience.

– **Threat- and incident-sharing and reporting** Sharing and analysis centres (ISACs) and utilities have become increasingly crucial for cross-border electricity entities – for example, Electricity (E-ISAC) in the US and European Energy (EE-ISAC) in Europe. However, current mechanisms for sharing incident and threat data have proven insufficient, particularly for utilities operating in multiple jurisdictions. In many cases, the rules defining which incidents require a report have been interpreted too narrowly, leading to very few incidents being reported.[17] Nonetheless, both the NERC CIP Standards and NIS Directive emphasize the importance of information-sharing – even though the results have been limited thus far. Moreover, the sharing of information must go beyond the subscription to information feeds and include active participation in public-private action groups with not only electricity companies, but also intelligence and law enforcement agencies.

Recommendations for the public and private sectors on laws and regulations

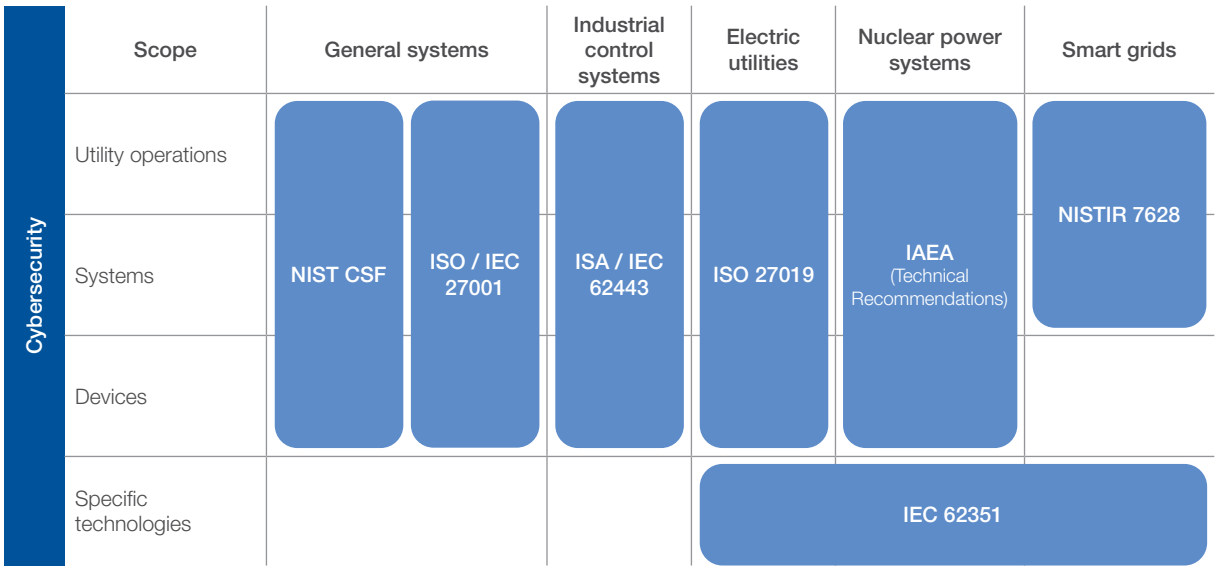
1. The guidance should call for regulators to mandate adherence to outcome-based cybersecurity frameworks such as those included in the UK CAF[18] and a corporate governance programme aligned with Board principles for cyber resilience published by the World Economic Forum[19] to address the key areas below:
   - Development of a comprehensive cyber-resilience programme covering organizational structure, policies, awareness, capabilities and processes, based on best practice frameworks such as NIST 800-53[20] and ISO 27001/2[21] to identify and mitigate the potential risks for the electricity sector, including emerging and supply-chain risks
   - Effective cybersecurity governance that embeds principles such as those defined by this community in 2019,[22] to ensure effective oversight of cyber risks by the Board
   - Implementation of applicable cybersecurity controls, protecting power grids and associated assets from cyberattack
   - Monitoring and detection of cybersecurity events and incidents accompanied by formalized procedures for efficient incident-handling and reporting
   - Minimization of impact from cybersecurity events and incidents, and formalized procedures for business continuity and disaster recovery, facilitating the rapid restoration of essential services
2. Utilities should periodically conduct risk assessments as threats and technology evolve, and ensure they are adhering to the controls defined for their cybersecurity programme.
3. Regulators worldwide should agree on global risk-based regulatory guidance to incorporate into their regulations to allow for consistent regulations across countries and regions, while retaining the flexibility to tailor their regulations in a way that reflects their national and ecosystem-specific interests. This guidance should also consider manufacturers and both small and large utilities.
4. Information-sharing programmes should be global in nature to address the international structures of many utilities and the threat landscape. These programmes should encourage sharing at appropriate levels between utilities, suppliers, integrators and government agencies. Sharing could include sanitized data on actual incidents, discovered vulnerabilities and indicators of compromise on detected threats.

3.0 Standards and frameworks overview

3.1 Global cybersecurity standards and technical recommendations

International cybersecurity standards operate at varying levels of detail, encompassing differing scopes. As Figure 4 illustrates, standards and frameworks commonly used by power utilities target different angles from operations to product selection to engineering. They were designed to overlap to a high degree, covering cybersecurity practices for people, processes and technologies (see Figure 4) with a focus on different disciplines by design.

FIGURE 4. REVIEWED STANDARDS AND FRAMEWORKS



3.2 Results of standards and frameworks analysis

Unlike laws and regulations with mandatory requirements, adherence to cybersecurity standards and frameworks is optional (except in a few cases where compliance is mandatory). Although both may be based on industry best practice, standards tend to be more rigid, whereas frameworks allow for more flexibility in implementation. Some of these standards are designed specifically for utilities, some cover operational technology for multiple industries, and others focus on information technology more broadly. Appendix B provides a more detailed description of the international cybersecurity standards reviewed. Based on a comprehensive review of the standards combined with collective workstream feedback, results showed:

- Current international cybersecurity standards are fit for purpose because they are intended for selective use where suitable in an environment.
- Together these cybersecurity standards can be leveraged to address a variety of challenges to the entire system and enterprise. They offer guidelines with mitigating security controls.
- None of the standards and frameworks reviewed are intended to be fully comprehensive solutions. They overlap and compensate, and to a large extent are based on very similar principles.

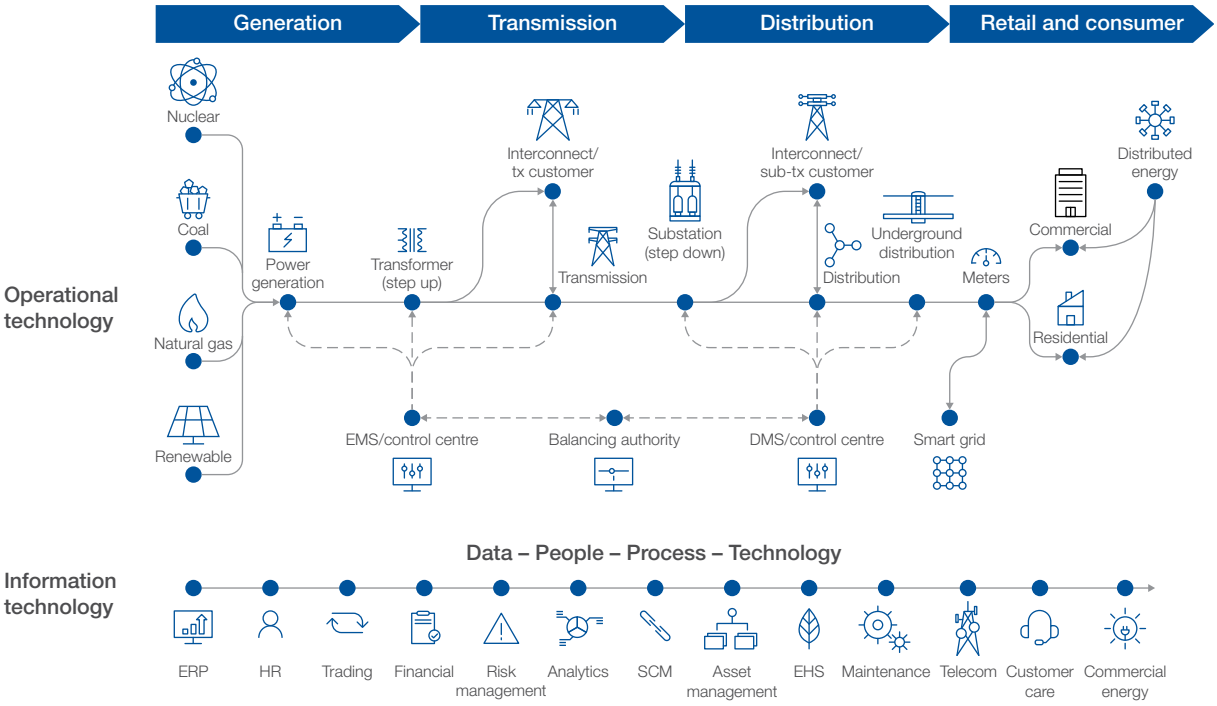
Recommendations for the public and private sectors on cybersecurity standards and frameworks

1. Utilities should selectively adopt provisions from various standards and frameworks where appropriate. Chosen approaches should cover interdependencies across the ecosystem, promoting collaboration and information-sharing.
2. Regulators should avoid making these standards compulsory in their entirety and instead use them and other cybersecurity frameworks as useful tools when designing a cybersecurity programme for specific operational aspects.
3. Utilities should follow reference architectures and product-specific implementation guidance, where relevant, when deploying or updating their systems. For example, the NIST Cybersecurity Center of Excellence offers several technology-specific use cases that can help security architects and engineers more efficiently design and deploy security tools and platforms for the energy sector.[23]

4.0 Product certification

As noted above, supply-chain risks continue to be a concern. While regulations such as the NERC CIP have started to adopt supply-chain requirements, the most significant missing piece has been an effective way for utilities to understand the security capabilities and risks associated with the products they buy. However, such a scheme is useful only when there is clearly defined guidance in place to apply it, such as that envisioned in articles 51–65 of the EU Cybersecurity Act.[24] As the power utility value chain depicted in Figure 5 illustrates, there are several interdependencies that need to be addressed to ensure that the associated processes continue to operate successfully and securely.

FIGURE 5. POWER UTILITY VALUE CHAIN



The following findings highlight that additional effort is required:

- There is no existing mechanism to provide security certification for products supporting power utilities. There have been some voluntary efforts to pursue certification under standards such as IEC 62443, but they have been very limited.

- Other existing certification schemes, except for common criteria for government buyers, depend on product vendors to voluntarily opt in for the certification, which they often use for marketing purposes. In some countries, for instance, Germany, utilities may be folded into the common criteria process. Still, such examples are limited and present their own challenges to extend a scheme to an industry with a different set of needs.

- There is no governing body to serve power utilities that could oversee the certification criteria, accredit certification labs or act as an arbiter in disputes. Product certifications may provide a limited view and may be insufficient in themselves. To obtain a comprehensive perspective, secure architectures also need to be considered.

Recommendations for the public and private sectors on product certification

1. Product certification processes for electric utilities should include the following:

   – **Governing body should approve certification criteria.** Voluntary industry groups involving utilities, product vendors, systems integrators and other interested parties should develop the actual criteria using a method similar to that used for developing international standards. An organization with some legal or contractual authority needs to act as a credible independent approver with the ability to serve as the ultimate arbiter of certification criteria, lest multiple competing certification criteria proliferate, as is the case today. Existing certification governing bodies could be used so long as the needs of utilities are adequately represented with appropriate schemes adopted. Additionally, any existing body would need sufficient subject-matter expertise about the electricity industry. This body could also accredit testing labs described below or use the existing accreditations granted to labs where appropriate.

   – **Key stakeholders within utilities should determine what products and systems need to be certified and why.** This will consist of members from an appropriately layered and chartered configuration/change control board (CCB), with representation from different functions (e.g. operations, legal, compliance, security and others) in collaboration with other utilities and regulators.

   – **Testing labs should confirm that products adhere to the certification criteria.** This is by far the most natural step as these firms exist in a significant number worldwide. The labs, which typically charge product vendors for testing, would usually maintain an accreditation, have their processes audited and report to the governing body described above. Many labs already exist that could perform this work with the appropriate schemes and oversight in place.

   – **An oversight body should ensure that utilities are purchasing only certified products or are granted waivers.** Typically, this role will be performed by a national electric utility regulator, potentially including reference to product certifications as an appendix to its risk assessment report. The exception-handling process, which will incorporate appropriate justification, may be a little more complicated because the local regulator may not have sufficient technical expertise to grant waivers. However, the governing body could potentially provide advisory services on the matter, with the local regulator having the final authority. While many certification schemes have the first three elements, the last one is rare due to legal and political ramifications.

2. Utilities and regulators globally should implement a certification programme incorporating the above elements that would create obligations on product suppliers to implement appropriate security controls in their products. Some countries have aspects of this scheme, but due to the global nature of electricity industry products, it is essential to build an international framework that offers consistency and transparency wherever possible.

5.0 Regulatory and related public-sector practices

Regulations may be written in a balanced way to properly incentivize appropriate cybersecurity behaviour while allowing utilities to adapt to threats and technological innovation. Yet a regulatory scheme can fail if the behaviour of those enforcing regulations or cooperative agreements does not apply a similar balance. Our research and feedback from workstream participants found that:

- Regulations make it possible to justify investments for the implementation of cybersecurity controls. The challenge is going beyond regulatory compliance to an approach focused on cyber resilience as a whole.

- The relationship between utilities and regulators may, at times, be contentious. Although some regulators may approach audits from the policing standpoint, others place a greater emphasis on outreach, education and collaboration.[25]

- Many utilities view audits as promoting a checkbox mentality that does not incentivize utilities to go beyond regulatory compliance requirements to achieve more mature cyber-resilience practices. These practices may also be costly and erode trust between the different parties.[26]

- In Europe, where fines and regular audits are not common, utilities have found the relationship with regulators to be less contentious than in North America.

- Through efforts such as the North American Transmission Forum (NATF)[27] and EU Cybersecurity Act of 2017,[28] mechanisms are developing to enforce appropriate cybersecurity practices through a more peer-based system of accountability. According to the 2019 Eurobarometer 492 survey,[29] conducted by the European Commission, approximately 86% of EU citizens agreed that cybersecurity collaboration between member states and utilities needs to be improved.

- Legally binding implementing regulations such as the upcoming Network Code for Cybersecurity[30] from the European Union will enable utilities to leverage peer-based accountability. This can be achieved by implementing the necessary controls based on those implemented by other utilities in support of the operation of transmission and distribution networks.

- There is a need for robust information-sharing mechanisms between different public- and private-sector actors in the electricity sector in order to share actionable information and mitigate cybersecurity risks effectively. Power utilities spanning national borders may find it challenging to receive and effectively disseminate information across their security organization due to national data sovereignty laws. While this is often an unavoidable reality of nation states, it nonetheless poses challenges for cross-border cooperation.

Recommendations for the public and private sectors on regulatory processes

1. Regulators should focus more on outcome-based principles and objectives and less on prescribing detailed security control requirements. This should be done in coordination with national security agencies and other government authorities that may have diverse interests.

2. The regulatory process should encompass inputs across government entities to align with the various stakeholders in national defence, law enforcement, commerce and other areas, and develop a common strategy to mitigate cybersecurity threats for essential services.

3. Regulatory oversight should exhibit flexibility to enable utilities to adapt to evolving threats and technological changes as well as to focus on people and processes. They should encourage an ecosystem-wide view with relevant interdependencies and collaboration, including the risks that different actors may add to the ecosystem.

4. Further research and surveys should be conducted to better understand the effects of regulations and to identify opportunities for improvement.

5. What appears to be missing at the country level is an emphasis on consensus guidance describing how utilities can effectively craft cybersecurity programmes, particularly for core functions supporting generation, transmission and distribution.

6. Strengthen trust-based information-sharing mechanisms between the public and private sectors to incentivize the exchange of information related to incidents, actionable insights and threat intelligence without the fear of repercussion.

6.0 Conclusion

The analysis and recommendations in this paper are intended to serve as a basis for further public-private dialogue and action. The North America and Europe Union regions were chosen as examples to illustrate and highlight areas for improvement in current policies.

Regulators across different regions would need to agree on aligned regulatory guidance, which both effectively mitigates risk and includes the ability to tailor regulations to reflect national interests. These practices should promote greater ecosystem-wide and cross-border collaboration in areas such as information-sharing, and encourage actionable information-sharing by private-sector actors, government entities and law enforcement agencies.

Furthermore, supply-chain risks continue to raise concern, as evidenced by the recent release of the US Presidential Executive Order. The power utility value chain includes several dependencies that should be addressed to ensure the safe, reliable operation of the electricity sector. Obtaining a more comprehensive perspective requires consideration of security architectures along with certification efforts.

With a shift towards promoting cyber resilience and a risk-based approach that focuses on outcomes, regulations will enable businesses in the electricity sector to allocate resources more efficiently, mitigate emerging risks related to the fast adoption of digital solutions and renewables, and achieve smarter, faster and more connected futures, driving growth and efficiency within the industry.

Glossary

Critical infrastructure: Critical infrastructure is the body of systems, networks and assets that are so essential that their continued operation is required to ensure the security of a given nation, its economy and the public's health and/or safety. Although critical infrastructure is similar in all nations due to the basic requirements of life, the infrastructure deemed critical can vary according to a nation's needs, resources and development level.[31]

Cyber resilience: Cyber resilience is the capacity of an organization to prepare, respond and recover when cyberattacks happen. An organization has cyber resilience if it can defend itself against these attacks, limit the effects of a security incident and guarantee the continuity of its operation during and after the attacks.[32]

Cybersecurity: Also referred to as information security, cybersecurity refers to the practice of ensuring the integrity, confidentiality and availability (ICA) of information. Cybersecurity is comprised of an evolving set of tools, risk-management approaches, technologies, training and best practices designed to protect networks, devices, programmes and data from attacks or unauthorized access.[33]

Industrial control system (ICS): An information system used to control industrial processes such as manufacturing, product handling, production and distribution. Industrial control systems include supervisory control and data acquisition systems used to manage geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.[34]

Industrial internet of things (IIoT): The industrial internet of things (IIoT) refers to the extension and use of the internet of things (IoT) in industrial sectors and applications. With a strong focus on machine-to-machine (M2M) communication, big data and machine learning, the IIoT enables industries and enterprises to have better efficiency and reliability in their operations.[35]

Information and communications technology (ICT): Information and communications technology (ICT) refers to all the technology used to handle telecommunications, broadcast media, intelligent building-management systems, audiovisual processing and transmission systems and network-based control and monitoring functions. Although ICT is often considered an extended synonym for information technology (IT), its scope is broader.[36]

Information technology (IT): Information technology (IT) covers any form of technology; that is, any equipment or technique used by a company, institution or any other organization that handles information.[37]

Operational technology (OT): Operational technology monitors and manages industrial process assets and manufacturing/industrial equipment. OT has existed much longer than IT or information technology, more specifically since people started to use machinery and equipment powered by electricity in factories, buildings, transportation systems, the utility industry, etc.[38]

Appendix A: IT–OT Convergence

Operational technology (OT) includes industrial control systems (ICSs) such as supervisory control and data acquisition (SCADA) devices, energy management systems (EMSs) and distributed control systems (DCSs), which monitor, control and access operational and industrial equipment. Programmable logic controllers (PLCs), used for automation and control, were initially used in the automotive sector, but have expanded into other industries, including electric utilities.

Historically, many OT ICSs, including those used in generation, transmission and distribution operations for electric utilities, used proprietary serial protocols for communication and customized operating systems and were "air-gapped", isolating them and mitigating risk from threat vulnerabilities found in information technology (IT) infrastructure. Therefore, they lack common cybersecurity controls such as authentication, encryption and other risk-mitigation measures common to the IT world.

However, beginning in the latter part of the 1990s, Transmission Control Protocol/Internet Protocol (TCP/IP) network capabilities began to grow in popularity for both IT and OT equipment.

Implementation of internet technology in OT environments like those used by electric utilities has provided a lower-cost alternative, including enhanced connectivity and compatibility with other devices. As a result, modern ICSs, which were never intended for connection to the internet, are now being manufactured and delivered with increasing built-in networking capabilities. This phenomenon, known as the industrial internet of things (IIoT), has opened new threat vectors and changed the vulnerability landscape of the electric grid, creating significant challenges accompanied by greater risks. Unlike traditional IT systems, compromises and failures of electric energy with IIoT devices could potentially lead to security and safety risks, endangering lives and damaging expensive equipment.

Appendix B: Legal and regulatory background

FIGURE 6. US AND EU LAWS/REGULATIONS

AREA	REGULATION/LAW
North America	US Energy Policy Act, Public Law 109-58, 8 August 2005, https://www.govinfo.gov/content/pkg/STATUTE-119/pdf/STATUTE-119-Pg594.pdf US NERC Critical Infrastructure Protection (CIP) Standards, https://www.nerc.net/standardsreports/standardssummary.aspx US Energy Independence and Security Act, Public Law 110-140, 19 December 2007, https://www.govinfo.gov/content/pkg/STATUTE-121/pdf/STATUTE-121-Pg1492.pdf US Executive Order: Improving Critical Infrastructure Cybersecurity, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0 US Presidential Policy Directive, United States Cyber Incident Coordination, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident Presidential Policy Directive – Critical Infrastructure Security and Resilience, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

AREA		REGULATION/LAW
North America		Cyber Security Plan for Nuclear Power Reactors, NEI 08-09, Nuclear Energy Institute, Revision 6, https://www.nrc.gov/docs/ML1011/ML101180437.pdf Identifying Systems and Assets Subject to the Cyber Security Rule, NEI 10–04, Nuclear Energy Institute, Revision 2 July 2012, https://www.nrc.gov/docs/ML1218/ML12180A081.pdf National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age, 2018, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf Executive Order on Securing the United States Bulk-Power System, White House, 1 May 2020, https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/
Europe	EU	"The Directive on Security of Network and Information Systems (NIS Directive)", European Commission, 6 July 2016, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act)", European Parliament, 17 April 2019, https://eur-lex.europa.eu/eli/reg/2019/881/oj "Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the Internal Market for Electricity", European Parliament, 5 June 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.158.01.0054.01.ENG "Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on Risk-Preparedness in the Electricity Sector and Repealing Directive 2005/89/EC", European Parliament, 5 June 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.158.01.0001.01.ENG "Directive 2005/89/EC of the European Parliament and of the Council of 18 January 2006 Concerning Measures to Safeguard Security of Electricity Supply and Infrastructure Investment", https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32005L0089 "Communication from the Commission on a European Programme for Critical Infrastructure Protection", 12 December 2006, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF "Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection", https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114 "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions", 2 July 2013, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667

AREA		REGULATION/LAW
Europe	Sweden	Security Protection Act (2018:585), https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddslag-2018585_sfs-2018-585
	Belgium	"Act 1 of July 2011 on the Security and Protection of Critical Infrastructures", Belgian Institute for Postal Services and Telecommunications, 1 July 2011, https://www.nbb.be/en/articles/law-1-july-2011-security-and-protection-critical-infrastructures-updated-25092018
	Germany	IT Security Act, Federal Law Gazette Year 2015 Part I No. 31, issued to Bonn on 24 July 2015 IT Security Catalog, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf?__blob=publicationFile&v=1
	Czech Republic	"Act No. 181 of 23 July 2014, Coll. of 23 July 2014 on Cybersecurity and Change of Related Acts (The Act on Cybersecurity)", Czech Republic Parliament, 23 July 2014, https://www.govcert.cz/download/kii-vis/preklady/Act_181_2014_EN_v1.0_final.pdf
	France	"Decree No. 2018–384, Transposition of the NIS Directive in France", French Parliament, 25 May 2018, https://www.ssi.gouv.fr/en/actualite/transposition-of-the-nis-directive-in-france/ "Law 2013/1168, Cybersecurity in France", Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), 10 December 2013, https://www.ssi.gouv.fr/en/cybersecurity-in-france/
	Spain	"Resolution of 8 September 2015, of Ministry of Security, Which Are Approved New Minimum Content of Operator Security Plans and Specific Protection Plans", Global Regulation, 8 September 2015, https://www.global-regulation.com/translation/spain/615585/resolution-of-8-september-2015%252c-of-the-ministry-of-security%252c-which-are-approved-new-minimum-content-of-the-operator-security-plans-and-specific-pr.html "Law 8/2011, 28 April, By Which Establish Measures for the Protection of Critical Infrastructure", https://www.global-regulation.com/translation/spain/1437394/law-8-2011%252c-28-april%252c-by-which-establish-measures-for-the-protection-of-critical-infrastructure.html
	Italy	Decreto Legislativo (DLGS) 65/2018, Decreto Legislativo 18 maggio 2018, n. 65, https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg Decreto Legislativo (DLGS) 133/2019, "Italy: New Provisions on National Cybersecurity Enter into Force", Library of Congress, 16 October 2019, https://www.loc.gov/law/foreign-news/article/italy-new-provisions-on-national-cybersecurity-enter-into-force/
	United Kingdom	Ofgem Guidance, "NIS Directive and NIS Regulations 2018: Ofgem Guidance for Operators of Essential Services", Ofgem, 30 November 2019, https://www.ofgem.gov.uk/publications-and-updates/nis-directive-and-nis-regulations-2018-ofgem-guidance-operators-essential-services "National Cyber Security Strategy 2016–2021", HM Government, 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf "Cyber Assessment Framework", National Cyber Security Centre, 30 September 2019, https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework

North America

The shift to digitization in recent years has increased the attack surface. In February 2002, the Nuclear Energy Institute (NEI) issued Order EA-02-026,[39] which included cybersecurity mitigation measures. This Order was followed by NEI 04-04,[40] for the implementation of cybersecurity programmes, including plant generation equipment, up to and including the first breaker from the main transformer to the switchyard breaker. The US Nuclear Regulatory Commission (NRC) endorsed NEI 04-04, which enables the NRC to provide oversight, inspect and enforce cybersecurity requirements. This includes the identification of critical assets as the basis for NRC inspection. However, according to the Federal Energy Regulatory Commission (FERC), compliance with NEI 04-04 is insufficient and not mandatory because it did not satisfy the mandate of the Energy Policy Act of 2005.[41]

NRC 10 CFR 73.54, known as the "cybersecurity rule",[42] was published in 2009, requiring adequate inspectable security to help mitigate the risk of cyberattacks against nuclear power plants. This regulation includes security controls for the protection of computers, networks and communications equipment. NEI 08-09[43] addresses cybersecurity plans for nuclear reactors. NEI 10-04,[44] per the requirements of 10 CFR 73.54, also guides the identification of critical cyber systems.

The North American Electric Reliability Corporation (NERC) released the initial version of the Critical Infrastructure Protection (CIP) standards in 2007. Within North America, NERC creates and enforces regulatory criteria approved by FERC. NERC CIP standards include exemptions for NRC-regulated facilities. However, facilities within those US nuclear generation plants (including structures, systems and components) that are not regulated by the NRC are subject to regulatory compliance under the NERC CIP regulatory standards.[45] Version 3 of these standards, which used a risk-based assessment methodology (RBAM) to categorize and assign critical cyber assets (CCAs), was replaced by NERC CIP Version 5/6/7 standards using high-, medium- and low-impact rating criteria based on net real power capability, starting in 2016.[46] NERC is continually revising and updating CIP regulatory criteria based on lessons learned.

Europe

The European Critical Infrastructure Protection Directive (2008/114/EC) of 8 December 2008[47] established a procedure for identifying, designating and protecting European Critical Infrastructures (ECI) in the energy and transport sectors. In 2013, the European Parliament requested increased cyber resilience for critical infrastructure,[48] followed by a 2016 proposal to increase the role of the EU Agency for Network Information Security (ENISA) to include strong cybersecurity and risk mitigation.[49]

As shown in Figure 6 above, there is currently no EU-wide baseline security level, and the NIS Directive is a mechanism comparable to what the International Atomic Energy Agency (IAEA) is using for nuclear security (including cybersecurity). The 2018 implementation deadline forced nation states to implement a system of national elements that will hopefully increase the level of protection for critical information assets and infrastructure based on principles with further refinements at the member-state level.

This less prescriptive piece of legislation emphasized the establishment of governance frameworks and cooperation groups; implementation of computer security incident response teams (CSIRTs); and identification of national competent authorities (NCAs) and single points of contact (SPoCs) for cybersecurity monitoring, reporting, incident response and cross-border coordination. Figure 6 provides a list of the nation states that have implemented protections based on the NIS Directive through a formal process. Many others have implemented similar laws that are not considered a full application of the Directive. For the current status of its implementation within each country, see https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive.

During March 2019, the European Commission issued cybersecurity recommendations for the energy sector to EU member states, addressing higher-level cybersecurity standards, real-time requirements, secure communications and the security of legacy systems and IoT devices.[50] The new EU Cybersecurity Act 2019/881, which covers topics beyond those in the NIS Directive,

was adopted by the European Parliament and European Council in April 2019,[51] creating the first voluntary EU cybersecurity certification framework, under the purview of ENISA, for information and communication technologies (ICT) products to be recognized by all member states. This Act addresses the activities of ENISA that will require enhanced training and awareness, threat-intelligence sharing and management of CSIRTs and cyber incidents. Additionally, it concentrates on ICT security certification and IoT technology, focusing on validating the integrity and applicability of security products, processes and services.

The NIS Directive tends to be less prescriptive and more principle-based, focused on ensuring that operators of essential services (OES), including utilities, establish governance frameworks and cooperation groups with other member states; implementation of CSIRTs; and identification of NCAs and SPoCs for cybersecurity monitoring, reporting, incident response and cross-border coordination.

One of the challenges Europe faces is a lack of clarity on the cybersecurity posture for many utilities. In contrast, the introduction of the NERC CIP standards followed some high-profile outages, albeit not ones that necessarily resulted from cybersecurity weaknesses.

Among EU member states, the situation is similar but with less data available to assess the overall security posture. For both North America and Europe, a compromise might seem appropriate, requiring utilities to self-report their security readiness through self-administered risk assessments (using a template rooted in the model regulation), based on control categories specified in a proposed global regulation.

In general, it appears that the European formula gives more deference to regulated entities, enabling them to identify and implement appropriate cybersecurity controls based on preliminary risk assessments prioritizing interventions and measures that take into consideration business and legislative objectives. One exception to this strategy is Ofgem guidance for UK-based utilities.[52]

Ofgem has been the joint competent authority for the NIS regulations, collaboratively working with the electricity sector to assist with scoping, self-assessments and the development of improvement plans, using a risk-based approach for the CAF, which enables utilities to leverage recognized industry standards for risk mitigation. Additionally, Ofgem's "economic" regulations include a framework allowing for cyber-resilience investment during the upcoming 2021–2029 price-control period.[53]

Appendix C: International Cybersecurity Standards

This analysis reviewed the following current security standards and frameworks:

- NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF), Version 1.1 (2018)[54]
- ISO/IEC 27001/27002:2013: Information Technology – Security Techniques – Code of Practice for Information Security Controls[55]
- ISO/IEC 27019:2017: Information Technology – Security Techniques – Information Security Controls for the Energy Utility Industry[56]
- ISA/IEC 62443 (various parts published between 2009 and 2019): Security for Industrial Automation and Control Systems[57]
- IEC 62351:2018: Power Systems Management and Associated Information Exchange – Data and Communications Security[58]
- NISTIR 7628 Revision 1 (2014): Guidelines for Smart Grid Cybersecurity[59]

In 2000, the Institute of Electrical and Electronics Engineers (IEEE) published standard 1402,[60] addressing Electric Power Substation Physical and Electronic Security. During that same year, International Organization for Standardization/ International Electrotechnical Commission (ISO/ IEC) 17799,[61] which evolved into the ISO/IEC 2700x series, including ISO/IEC 27001/27002, was first published.

The IEC published report 62210 in 2003,[62] focusing on Data and Communications Security, including "common criteria" protection profiles. This report was followed in 2005 by ISO/IEC 15408,[63] which concentrated on application layer cryptographic protection profiles for communications between control centres and substations, including key management and end-to-end security. American National Standards Institute/International Society for Automation ANSI/ISA-99[64] provided the roots for the ISA/IEC-62443 series.

The IEC 62351 series, first published in 2007, focused on power systems security from a system and product design perspective, with a significant emphasis on providing the security underpinnings for the IEC 61850 (Communication Networks and Systems for Power Utility Automation and Associated Messaging Protocols)[65] and IEC 60870 (Relating to Transmission and Tele-Control Protocols such as the Inter-Control Center Communications Protocol [ICCP]).[66]

The NIST Cybersecurity Framework (CSF), first published in 2014, addresses cybersecurity for critical infrastructure and has become widely adopted as a standard throughout several industry sectors. The NIST CSF is a broad-based approach referencing more specific standards, focusing more on operational and governance considerations than technical architecture or product design. ISO 27001 provides a similar broad process-based view that may be supplemented by ISO 27019 to add a cybersecurity for utilities "flavour".

Different parts of the IEC 62443 series focus on OT from the policies and procedures, system and component perspectives, which may benefit asset owners, systems architects, product developers and others. The IEC 62351 series contains policies and procedures emphasizing system and component design and assessment, rooted in the security underpinnings of IEC 61850 and IEC 60870.

The NIST Interagency or Internal Reports (NISTIR) 7628, released in 2010, is a catalogue of smart grid security best practices that can be used selectively where appropriate. This documentation provides an analytical framework for developing effective cybersecurity strategies tailored for "smart" electrical grid characteristics, risks and vulnerabilities.

Contributors

Lead authors

Gib Sorebo	Senior Manager, Accenture Security
Thomas Duffey	Manager, Accenture Security

Working group co-chairs

Pierre-Alain Graf	Senior Vice-President, Global Security, ABB
Rosa Kariger	Global Chief Information Security Officer, Iberdrola

Advisory team

Louise Anderson	Community Lead, Electricity Industry, World Economic Forum
Georges de Moura	Head of Industry Solutions, Centre for Cybersecurity, World Economic Forum
Kristen Panerali	Head of Electricity Industry, World Economic Forum
Floris van den Dool	Managing Partner, Accenture

Working group

David Batz	Senior Director, Cyber and Infrastructure Security, Edison Electric Institute (EEI)
Christophe Blassiau	Senior Vice-President, Digital Security and Global Chief Information Security Officer, Schneider Electrics
Mario Bocchiola	Head of Operation Technology Cyber Security Engineering, Enel
Stefano Bracco	Knowledge Manager, Agency for the Cooperation of Energy Regulators
Andrea Brackett	Vice-President and Chief Information Security Officer, Tennessee Valley Authority
Felicia Brown	Chief Security Officer, Vice-President Physical and Cyber Security, Avangrid (Iberdrola)
Manny Cancel	Senior Vice-President and Chief Executive Officer of E-ISAC, North American Electric Reliability Corp
Kenneth Carnes	Vice-President and Chief Information Security Officer, New York Power Authority
Dexter Casey	Chief Information Security Officer, Centrica
Francesco Ciancarelli	Head of Cyber Security Standards and External Stakeholders, Enel
Tim Conway	Director of SCADA and ICS, Sans Institute
Lynn Costantini	Deputy Director Center for Partnerships and Innovation, National Association of Regulatory Utility Commissioners
Ivan Dragnev	Cyber Security Principal Technical Lead Europe, Electric Power Research Institute
Ashtad Engineer	Vice-President of Technology and Digitization, Adani Group
Hala Furst	Director of Cybersecurity and Innovation, US Department of Homeland Security, USA
Anielo Gentile	Cyber Security Manager, Enel
Agustin Valencia Gil-Ortega	Head of OT Cybersecurity, Iberdrola
Guido Gluschke	Director, Institute for Security and Safety (ISS)
Juha Harkonen	Vice-President Security, Fortum Corporation, Finland
Harshul Joshi	Cybersecurity Partner, PwC
Kai Hermsen	Global Coordinator for the Charter of Trust, Siemens
Martin Knudsen	Lead Information Security Officer, Ørsted
Michaela Kollau	Policy Officer, Directorate General for Energy, European Commission
Paulo Moniz	Director, Information Security and IT Risk, EDP
Scott Pinkerton	Cyber Security Programme Manager, Argonne National Laboratory
Philip Quade	Chief Information Security Officer, Fortinet

Johan Rambi	Faculty Instructor, Saxion University of Applied Sciences
Yuri Rassega	Chief Information Security Officer, Enel
Jesus Sanchez	Head of Global Cybersecurity, Naturgy
Leo Simonovich	Vice-President and Global Head, Industrial Cyber and Digital Security, Siemens
Eric Singer	Chief Information Security Officer, EMEA, Schneider Electrics
Cole Sinkford	Chief Information Security Officer, GE Renewable Energy
Vlada Spasic	Senior Advisor, SV Energy
Candace Suh-Lee	Principal Technical Leader – Cyber Security, EPRI (Electric Power Research Institute)
Eric Trapp	Chief Security Officer, Sempra Energy
Maximilian Urban	Information Security Officer and Innovation Manager, Netz Niederösterreich
Alain Vallieres	Cyber Security Manager, Hydro Quebec
Olivier Vandelaer	Director Industrial Cybersecurity, ENGIE Laborelec
Matt Wakefield	Director of Information, Communication and Cyber Security, Electric Power Research Institute
Swantje Westpfahl	Co-Director, Institute for Security and Safety (ISS)
Thomas Wilson	Senior Vice-President and Chief Information Security Officer, Southern Company
Brecht Wyseur	Product Manager, IoT Security, Kudelski Group
Mohammed Zumla	Head of Cyber Security and Resilience, NIS Competent Authority, Office of Gas and Electricity Markets (Ofgem)

Endnotes

1. See World Economic Forum, “Systems of Cyber Resilience: Electricity Workshop”, New York, 2019.

2. See IT Governance, “Cyber Resilience”, https://www.itgovernance.co.uk/cyber-resilience (link as of 16 June 2020).

3. See World Economic Forum, “The Global Risks Report 2020”, 15th edition, 2020, https://www.weforum.org/reports/the-global-risks-report-2020 (link as of 16 June 2020).

4. Ibid.

5. See World Economic Forum, “Systems of Cyber Resilience: Electricity”, https://www.weforum.org/projects/systems-of-cyber-resilience-electricity (link as of 16 June 2020).

6. See North American Electric Reliability Council, “(Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1”, 2006, https://www.nerc.com/pa/Stand/Cyber%20Security%20Permanent/Revised_Implementation_Plan_CIP-002-009.pdf (link as of 16 June 2020).

7. See European Commission, “The Directive on Security of Network and Information Systems (NIS Directive)”, 6 July 2016, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (link as of 16 June 2020).

8. Earlier EU-wide legislation included the “Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection”, European Council, 8 December 2008, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114 (link as of 16 June 2020).

9. See European Commission, “The Directive on Security of Network and Information Systems (NIS Directive)”, 6 July 2016, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (link as of 16 June 2020).

10. See Arnault Barichella, “Cybersecurity in the Energy Sector: A Comparative Analysis between Europe and the United States”, Études de l’Ifri, February 2018, https://www.ifri.org/en/publications/etudes-de-lifri/cybersecurity-energy-sector-comparative-analysis-between-europe-and (link as of 16 June 2020).

11. See, e.g., Utility Dive, “Duke fined $10m for Cybersecurity Lapses Since 2015”, 4 February 2019, https://www.utilitydive.com/news/duke-fined-10m-for-cybersecurity-lapses-since-2015/547528/ (link as of 16 June 2020). The fine was imposed even though no security breaches were ever tied to these violations.

12. See Luke Irwin, “NIS Directive and GDPR Double Jeopardy: Can You Be Fined Twice for the Same Breach?”, IT Governance, 27 April 2018, https://www.itgovernance.co.uk/blog/nis-directive-and-gdpr-double-jeopardy-can-you-be-fined-twice-for-the-same-breach, noting that “the maximum penalties will likely only be handed out for flagrant or repeat offences, and the UK government has said that fines will be a last resort” (link as of 16 June 2020).

13. See National Cyber Security Centre, “NCSC CAF Guidance: Introduction to the Cyber Assessment Framework”, https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework; see also Information Commissioner’s Office, “The Information Commissioner’s Response to the Ofgem Consultation Standards of Conduct for Suppliers in the Retail Energy Market”, 13 March 2017, https://www.ofgem.gov.uk/ofgem-publications/117734 (links as of 16 June 2020).

14. See North American Electric Reliability Corporation, “CIP-013-1 – Cyber Security – Supply Chain Risk Management”, https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf (link as of 16 June 2020).

15. For example, the latest version of the NIST cybersecurity framework, version 1.1, includes an expanded section 3.3 with a discussion of supply-chain risk that explains how to communicate risks to all levels of the supply chain. However, that is still rather high level. In general, guidance seems to currently fall into two categories: broad-based guidance that simply calls for some vetting of suppliers or specific bans on individual suppliers – with little in between.

16. See US White House, "Executive Order on Securing the United States Bulk-Power System", 1 May 2020, https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/ (link as of 16 June 2020).

17. See Federal Energy Regulatory Commission (FERC), Docket No. RD19-3-000, https://elibrary.ferc.gov/idmws/common/OpenNat.asp?fileID=15278927 ("In its petition, NERC states that proposed Reliability Standard CIP-008-6 broadens the mandatory reporting of Cyber Security Incidents and thus addresses the concern that currently-effective Reliability Standard CIP-008-5 may not encompass the full scope of cyber-related threats to the Bulk-Power System.") This action by NERC that FERC approved was in response to an earlier FERC request, which expressed concern about "lack of Reportable Cyber Security Incidents in 2015 and 2016". See FERC Order No. 848, https://www.ferc.gov/whats-new/comm-meet/2018/071918/E-1.pdf (links as of 16 June 2020).

18. See National Cyber Security Centre (NCSC), "NCSC Cyber Assessment Framework Guidance", https://www.ncsc.gov.uk/collection/caf (link as of 16 June 2020).

19. See World Economic Forum, "Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards", January 2019, https://www.weforum.org/whitepapers/cyber-resilience-in-the-electricity-ecosystem-principles-and-guidance-for-boards/ (link as of 16 June 2020).

20. NIST, "Security and Privacy Controls for Information Systems and Organizations (Final Public Draft)", March 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft (link as of 22 June 2020).

21. ISO, "ISO/IEC 27001: Information Security Management", https://www.iso.org/isoiec-27001-information-security.html (link as of 22 June 2020).

22. Ibid.

23. See National Cybersecurity Center of Excellence (NCCE), "Energy Sector", https://www.nccoe.nist.gov/projects/use-cases/energy-sector (link as of 16 June 2020).

24. For a discussion on current efforts on building a certification framework in the EU information and communications technology (ICT) products, services and processes, including formation of the Stakeholder Cybersecurity Certification Group, see European Commission, "The EU Cyber Security Certification Framework", https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (link as of 16 June 2020). This voluntary scheme, which is intended to be adopted by individual member states, calls for a comprehensive structure to set security standards for products and evaluate them to ensure they are free from known vulnerabilities, that they are "secure by default and by design" and that there are secure and reliable update mechanisms.

25. For a useful perspective on NERC CIP regulatory practices from the regulator's point of view, see H. T. Duffey "Exploring the Impact of NERC CIP Regulatory Compliance on Risk and Security for Bulk Electric System Grid Cyber-Attacks: A Qualitative Phenomenological Study", doctoral dissertation, Northcentral University, December 2018.

26. For a better understanding of the issue, see Marlene Z. Ladendorff, "The Effect of the NERC CIP Standards on the Reliability of the North American Bulk Electric System", The ICER Chronicle, June 2016.

27. North American Transmission Forum website, https://www.natf.net/ (link as of 18 June 2020).

28. See European Commission, “The EU Cybersecurity Act”, 28 February 2020, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act (link as of 16 June 2020).

29. See European Commission, “Special Eurobarometer 464a: Europeans Attitudes toward Cybersecurity”, September 2017.

30. See Smart Grid Task Force Expert Group 2 (SGTF EG2) Cybersecurity, “Interim Report: Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity”, December 2017.

31. See TechTarget, “Critical infrastructure”, https://whatis.techtarget.com/definition/critical-infrastructure (link as of 16 June 2020).

32. See RSI Security, “What Is Cyber Resilience and Why Is It Important?”, 14 August 2019, https://blog.rsisecurity.com/what-is-cyber-resilience-and-why-is-it-important/ (link as of 16 June 2020).

33. See Forcepoint, “What is Cybersecurity?”, https://www.forcepoint.com/cyber-edu/cybersecurity (link as of 16 June 2020).

34. See National Institute of Standards and Technology, “Industrial Control System (ICS) – Definition”, https://csrc.nist.gov/glossary/term/industrial_control_system (link as of 16 June 2020).

35. See Trend Micro, “Industrial Internet of Things”, https://www.trendmicro.com/vinfo/us/security/definition/industrial-internet-of-things-iiot (link as of 16 June 2020).

36. See Asociación Europe You, “What is Information and Communication Technology?”, http://europeyou.eu/es/what-is-information-and-communication-technology/ (link as of 16 June 2020).

37. See Science Direct, “Information Technology”, https://www.sciencedirect.com/topics/computer-science/information-technology (link as of 16 June 2020).

38. See i-scoop, “Operational Technology (OT) – Definitions and Differences with IT”, https://www.i-scoop.eu/industry-4-0/operational-technology-ot/ (link as of 16 June 2020).

39. See Nuclear Regulatory Commission, “EA-02-026 – Safeguards Information: Issuance of Order for Interim Safeguards and Security Compensatory Measures for [Plant name]”, https://www.nrc.gov/reading-rm/doc-collections/enforcement/security/2002/security-order-2-25-02.pdf (link as of 16 June 2020).

40. See Nuclear Energy Institute, “NRC Staff Review of NEI 04-04, Cyber Security Program for Power Reactors, Revision 2”, 6 August 2007, https://www.nrc.gov/docs/ML0724/ML072420407.pdf (link as of 16 June 2020).

41. See United States Environmental Protection Agency, “Summary of the Energy Policy Act”, https://www.epa.gov/laws-regulations/summary-energy-policy-act (link as of 16 June 2020).

42. See Nuclear Regulatory Commission, “NRC 10 CFR 73.54 – Protection of Digital Computer and Communication Systems and Networks”, 2 November 2015, https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html (link as of 16 June 2020).

43. See Anastasios Arampatzis, “State of Security: What Is NEI 08-09?”, Tripwire, 15 October 2019, https://www.tripwire.com/state-of-security/ics-security/what-is-nei-08-09 (link as of 16 June 2020).

44. See Nuclear Energy Institute, “NEI 10-04 – Identifying Systems and Assets Subject to the Cyber Security Rule”, July 2012, https://www.nrc.gov/docs/ML1218/ML12180A081.pdf (link as of 16 June 2020).

45. See Washington Energy Report, "FERC Accepts NERC's Implementation Plan Regarding CIP Standards", Troutman Sanders, 26 March 2010, https://www.troutmansandersenergyreport.com/2010/03/ferc-accepts-nercs-implementation-plan-regarding-cip-standards/ (link as of 16 June 2020).

46. See North American Electric Reliability Corporation, "CIP Standards".

47. See European Council, "Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection", 8 December 2008, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114 (link as of 16 June 2020).

48. See European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", 7 February 2013, https://ec.europa.eu/home-affairs/what-is-new/news/news/2013/20130207_01_en (link as of 16 June 2020).

49. See EU Cyber Security Agency, "ENISA Strategy 2016–2020", January 2016, https://www.enisa.europa.eu/publications/corporate/enisa-strategy (link as of 16 June 2020).

50. See European Commission, "Commission Recommendation of 3.4.2019 on Cybersecurity in the Energy Sector", 4 March 2019, https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf (link as of 16 June 2020).

51. See European Commission, "The EU Cybersecurity Act", 28 February 2020, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act (link as of 16 June 2020).

52. See Ofgem, "NIS Directive and NIS Regulations 2018: Ofgem Guidance for Operators of Essential Services", 30 November 2019, https://www.ofgem.gov.uk/publications-and-updates/nis-directive-and-nis-regulations-2018-ofgem-guidance-operators-essential-services (link as of 16 June 2020).

53. See Ofgem, "RIIO-2 Cyber Resilience Guidelines", 5 February 2020, https://www.ofgem.gov.uk/publications-and-updates/riio-2-cyber-resilience-guidelines (link as of 16 June 2020).

54. See National Institute of Standards and Technology, "Cybersecurity Framework", https://www.nist.gov/cyberframework (link as of 16 June 2020).

55. See International Organization for Standardization/International Electrotechnical Commission, "ISO/IEC 27001:2013 Information Security Management", https://www.iso.org/isoiec-27001-information-security.html (link as of 16 June 2020).

56. See International Organization for Standardization/International Electrotechnical Commission, "ISO/IEC 27019:2017 [ISO/IEC 27019:2017] Information Technology – Security Techniques – Information Security Controls for the Energy Utility Industry", https://www.iso.org/standard/68091.html (link as of 16 June 2020).

57. See International Society of Automation/International Electrotechnical Commission, "New ISA/IEC 62443 Standard Specifies Security Capabilities for Control System Components", September–October 2018, https://www.isa.org/intech/201810standards/ (link as of 16 June 2020).

58. See International Electrotechnical Commission, "IEC 62351:2020 Power Systems Management and Associated Information Exchange – Data and Communications Security", https://webstore.iec.ch/publication/6912 (link as of 16 June 2020).

59. See National Institute of Standards and Technology Computer Security Resource Center, "NISTIR 7628 Rev. 1 Guidelines for Smart Grid Cybersecurity", https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final (link as of 16 June 2020).

60. See Institute of Electrical and Electronics Engineers, “IEEE 1402-2000 – IEEE Guide for Electric Power Substation Physical and Electronic Security”, https://standards.ieee.org/standard/1402-2000.html (link as of 16 June 2020).

61. See International Organization for Standardization/International Electrotechnical Commission, “ISO/IEC 17799:2005 [ISO/IEC 17799:2005] Information Technology – Security Techniques – Code of Practice for Information Security Management”, https://www.iso.org/standard/39612.html (link as of 16 June 2020).

62. See International Electrotechnical Commission, “IEC TR 62210 Power System Control and Associated Communications – Data and Communication Security”, https://webstore.iec.ch/preview/info_iec62210%7Bed1.0%7Den.pdf (link as of 16 June 2020).

63. See International Organization for Standardization/International Electrotechnical Commission, “ISO/IEC 15408-1:2009 [ISO/IEC 15408-1:2009] Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and General Model”, https://www.iso.org/standard/50341.html (link as of 16 June 2020).

64. See American National Standards Institute/International Society of Automation, “ISA99 – Industrial Automation and Control Systems Security”, https://www.isa.org/isa99/ (link as of 16 June 2020).

65. See ABB, “IEC 61850 Power Utility Automation”, https://new.abb.com/substation-automation/systems/iec-61850 (link as of 16 June 2020).

66. See International Electrotechnical Commission, “IEC 60870-5:2020 Series – Telecontrol Equipment and Systems”, https://webstore.iec.ch/publication/3755 (link as of 16 June 2020).

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744

contact@weforum.org
www.weforum.org