Digitalization of security in the energy sector: evolution of EU law and policy

Mikko Rajavuori* and Kaisa Huhta**

ABSTRACT

This article analyses the dynamics and implications of the digitalization of security in the energy sector. Based on an evolutionary review of legal and policy instruments, we map the pace and internal dynamics of the digitalization of security in the European Union over the past 15 years. Our analysis reveals substantial changes in the conceptions and dynamics of security in the energy sector. First, we find that digitalization has only recently penetrated into the core of the energy sector’s security paradigm. Secondly, we uncover a significant disconnect in the conceptualization of the risk as against the opportunities associated with digitalization. Thirdly, we identify the growing influence of cross-sectoral instruments in the energy sector. Fourthly, we find that energy security does not feature in the overarching security discourse relating to the use of data-driven technologies in the energy sector. The findings illustrate the difficulties that managers, policymakers and researchers face when trying to keep up with the rapid technological change in the energy transition and the ensuing evolution of the energy sector’s security paradigm.

1. INTRODUCTION

Background and research objective

Digitalization has changed global society. Over the past few decades, the rise of digital data and data-driven technologies has recalibrated everyday life, industry and public discourse.1 While often equated with significant opportunities for positive technological disruption, digitalization has also changed our understanding of personal and public security. Following the rapid development of digital technologies from the late 1970s onwards, novel digital risks stemming from the interconnectedness between physical and virtual services and, more recently, the exploitation of massive data sets have joined traditional physical security threats, such as wars or natural disasters.2 As society’s reliance on digital and data-driven technologies has grown, many conventional security paradigms have been refined to include issues such as control over data, the resilience of information systems and overall technological development capacity. Security has digitalized.

* Mikko Rajavuori, Law School, Center for Climate Change, Energy and Environmental Law, University of Eastern Finland, Joensuu, Finland. Email: mikko.rajavuori@uef.fi
** Kaisa Huhta, Law School, Center for Climate Change, Energy and Environmental Law, University of Eastern Finland, Joensuu, Finland. Email: kaisa.huhta@uef.fi

This work was supported by the Academy of Finland [grant number 324037].

1 ME Porter and JE Heppelmann, ‘How Smart, Connected Products Are Transforming Companies’ (2015) 93 Harvard Business Review 96; JS Brennen and D Kreiss, ‘Digitalization’ in The International Encyclopedia of Communication Theory and Philosophy (John Wiley & Sons 2016).

2 J Eriksson and G Giacomello, International Relations and Security in the Digital Age (Routledge 2007); B Schneier, Secrets and Lies: Digital Security in a Networked World (John Wiley & Sons 2015).
The energy sector is no exception. As is widely acknowledged, the sector is undergoing a fundamental transformation towards a low-carbon design, which, among other things, includes an increase in variable, distributed renewable energy, energy efficiency, flexible demand, energy storage facilities and sector coupling, all of which hinge on data-driven technologies and solutions. Following the rapid digitalization that has taken place in different segments of the energy value chain, the sector's impending digital security concerns, ranging from the cybersecurity of energy systems to privacy in smart systems and ultimately to geostrategic competition in energy technology, have permeated public and private domains both nationally and internationally. Yet the dynamics of the 'digitalization of security' in the energy sector remain poorly understood.

This article analyses the dynamics and implications of the digitalization of security in the energy sector in the European Union (EU). Based on an evolutionary review of legal and policy instruments, we map the pace and internal dynamics of the digitalization of security in the EU over the past 15 years. Taking the changes in the overarching security paradigm as our starting point, our objective is to trace the gradual evolution in the conceptions of security in the energy sector as a range of digital risks and concerns prompted by the development of data-driven technologies have recently been added to traditional notions concerning such issues as security of supply.

Our analysis reveals substantial changes in the conceptions and dynamics of security in the energy sector. First, we note that digitalization penetrated only recently into the core of the energy sector's security paradigm. Secondly, we uncover a significant disconnect in the conceptualization of the risk as against the opportunities associated with digitalization. Thirdly, we identify the growing influence of cross-sectoral instruments in the energy sector. Fourthly, we find that energy security does not feature in the overarching security discourse relating to the use of data-driven technologies in the energy sector.

Data and methodology

The digitalization of security is an elusive concept. Depending on the level on which the analysis focuses, the security implications of digitalization may range from the theft of personal or company data to protecting vital network infrastructure and, increasingly, to guaranteeing the digital and technological sovereignty of a nation. Accordingly, the study of digital security has evolved into a vibrant and broad-based field of policy, business and research that covers disciplines as diverse as management, information technology, security studies, international relations and law. In the energy sector alone, the security implications of digitalization are addressed through the lenses of the cybersecurity of various energy systems and infrastructures as well as through the screening of foreign investments in critical energy technologies and with reference to privacy concerns. In addition, energy features prominently in traditional defence-orientated security policy, where...
the vulnerabilities of the digitalized energy sector, for example to hostile cyberoperations, are increasingly foregrounded.11

Due to its disciplinary breadth, complexity and technology-driven developmental path, an exhaustive analysis of the digitalization of security is beyond the scope of this article. Instead, we explore the dynamics and implications of the new digital security paradigm for the energy sector through a narrower lens. Substantively, we limit our analysis to EU law and policy instruments that impinge on the digitalization of security in the energy sector. Therefore, analysis of ‘hard’ security policies, such as the EU’s Common Security and Defence Policy, lies outside the scope of this article. Thematically, we focus on critical digital infrastructure. The protection of critical infrastructures, such as energy, water and transport facilities, has been a mainstay of traditional security policy for over two decades.12 More recently, however, the protection of digital or virtual infrastructure encompassing not only information and communications technologies but also big data, virtual platforms and cloud services has been added to this.13 We submit that assessment of the EU law and policy experience in relation to the evolution of critical digital infrastructure offers insights into the digitalization of security in the energy sector that have sectoral, cross-sectoral and international relevance.

In practice, we carry out an evolutionary content analysis in respect of 40 EU law and policy instruments that have been introduced over the past 15 years. By reference to the gradually increasing references to and focus on the protection of critical digital infrastructure in official EU sources, including legislation, policy documents and reporting by various EU bodies over time, we map the evolution of the digitalization of security in the EU energy sector. The policy and legal documents have been gathered and mapped based on their references to two or more of the following issues: energy, digitalization, data-driven technologies, security and physical, digital and critical infrastructures. Evolutionary analysis of these documents is augmented by traditional doctrinal legal approaches and supported by key literature in the intersection between energy and information and communications technology (ICT) law and policy.

Even though the digitalization of security in the energy sector affects individuals, companies and states globally, this article focuses on the evolution of EU law and policy. There are three reasons for this. First, energy and security have been at the core of the EU’s legal and policy measures from the beginning of European integration. The protection of energy infrastructures and technologies has historically assumed a central role in the development of the polity and, accordingly, the recent digitalization of security in the energy sector can be seen as a continuation of the earlier paradigms.14 Secondly, due to its unique institutional structure, EU law and policy essentially aggregate the conceptions of the digitalization of security across 27 Member States. In this way, the analysis of the EU instruments also serves to approximate various national responses. Finally, the rapid bottom-up digitalization of the EU energy markets has prompted regulatory responses that cover various segments of the energy value chain, including cybersecurity and data protection. For these reasons, we contend that assessment of the EU law and policy in this area is illustrative of broader developments in respect of the digitalization of security in the energy sector and provides vital benchmarks for other jurisdictions.

This article is structured as follows. Section 2 traces the emergence of the concept of critical digital infrastructure in EU law and policy instruments over the past 15 years. Taking these developments as illustrative of the broader trajectories in the digitalization of security, the section suggests that the protection of critical digital infrastructure has penetrated into the core of EU law and policy only in the past few years. Section 3

11 AM Berger, ‘The End of the War as We Know It: How an Act of Cyber Warfare Could Impact the US Energy Grid’ (2017) 22 Journal of Technology Law & Policy 141.
12 JD Moteff, ‘Critical Infrastructures: Background, Policy, and Implementation’ (2015) <https://fas.org/sgp/crs/homesec/RL30153.pdf>, accessed 1 October 2020.
13 T Kiravuo and others, ‘Peeking under the Skirts of a Nation: Finding Ics Vulnerabilities in the Critical Digital Infrastructure’ European Conference on Cyber Warfare and Security (Academic Conferences International Limited 2015).
14 J Snell and E Aalto, ‘Security and Integration in the Context of the Internal Market’ in Fabian Amtenbrink and others (eds), The Internal Market and the Future of European Integration (CUP 2019).
moves the focus onto the energy sector and regulatory tools designed to respond to new digital risks and concerns. Focusing on critical digital infrastructure, Section 3 traces the gradual move from a security paradigm based on the protection of physical energy assets to one that encompasses a range of digital infrastructures. Most importantly, the section highlights the urgency with which digitalized security concerns have been approached and mitigated over the past few years as well as the interplay between sectoral regulation and the new EU-wide cross-sectoral instruments. Section 4 concludes by summarizing the lessons that experience in relation to the digitalization of security within the EU’s energy sector offer for EU law and policy more broadly.

2. CRITICAL DIGITAL INFRASTRUCTURE: INSIGHTS INTO THE DIGITALIZATION OF SECURITY

The conceptual origins of critical infrastructure and critical digital infrastructure

Throughout the article, we adopt the perspective that assessment of the protection of critical digital infrastructure within the EU offers insights into the digitalization of security in the energy sector in a broader sense. The trajectory of critical infrastructure protection from the first established uses of the term in the mid-1990s to the current focus on critical digital infrastructure illustrates the pervasive influence of digitalization on the development of broader security paradigms.

There is no generally accepted cross-disciplinary or cross-jurisdictional definition of the term ‘critical infrastructure’.15 It is, however, generally used to refer to a range of small- and large-scale, interdependent systems vital for the functioning of society, defence and national security.16 Critical infrastructure protection has a long history, but it emerged both conceptually and as a focal point of security policy in the USA in the mid-1990s.17 Originally, foundational critical infrastructures were mostly limited to such areas as energy, finance, transportation, vital human services and telecommunications, but the concept has since then expanded to cover critical materials and other inputs. Designed as a cross-cutting tool to align various levels of public and private security, the protection of critical infrastructures became mainstream in law and policy in the USA, EU and many other parts of the world in the 2000s.18 In the EU, for instance, critical infrastructure emerged in policy discussions as a response to the rising threat of terrorist acts in 2004.19

As the inclusion of telecommunications as a key critical infrastructure suggests, communication networks and capabilities have long been considered vital for the functioning and security of society.20 Over time, however, the relative importance of digital technologies for the operation and functioning of critical infrastructure has increased.21 As the overall reliance on digital communication has grown, various digital and communication technologies have also entered into use to run most physical systems, ranging from traffic to water

15 C Alcaraz and S Zeadally, ‘Critical Infrastructure Protection: Requirements and Challenges for the 21st Century’ (2015) 8 International journal of critical infrastructure protection 53.
16 TG Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation (John Wiley & Sons 2019).
17 S Collier and A Lakoff, ‘The Vulnerability of Vital Systems: How “Critical Infrastructure” Became a Security Problem’ in MA Dunn and KS Kristensen (eds), Securing the Homeland: Critical Infrastructure, Risk and (In)Security (Routledge 2008)
18 AA Ghorbani and E Bagheri, ‘The State of the Art in Critical Infrastructure Protection: A Framework for Convergence’ (2008) 4 International Journal of Critical Infrastructures 215; Lewis (n 16).
19 Commission Communication, ‘Critical Infrastructure Protection in the Fight Against Terrorism’ COM (2004) 702 final; C Pursiainen, ‘The Challenges for European Critical Infrastructure Protection’ (2009) 31 European Integration 721.
20 GA Gow, Policymaking for Critical Infrastructure: A Case Study on Strategic Interventions in Public Safety Telecommunications (Routledge 2005).
21 C Wagner and others, ‘Impact of Critical Infrastructure Requirements on Service Migration Guidelines to the Cloud’ 2015 3rd International Conference on Future Internet of Things and Cloud (IEEE 2015); Z Nyikes and Z Rajnai, ‘Big Data, as Part of the Critical Infrastructure’ 2015 IEEE 13th International Symposium on Intelligent Systems and Informatics (SISY) (IEEE 2015); T Simon, ‘Critical Infrastructure and the Internet of Things’ (2017) Global Commission on Internet Governance Paper Series No 46 <https://www.cigionline.org/sites/default/files/documents/GCIG_no.46_0.pdf> accessed 1 October 2020.
Beyond providing an interconnected operational layer for various critical infrastructures, the most recent data-driven technologies are used to automate, integrate and optimize their operation.\footnote{JM Yusta, GJ Correa and R Lacal-Arántegui, ‘Methodologies and Applications for Critical Infrastructure Protection: State-of-the-Art’ (2011) 39 Energy Policy 6100.} The contemporary state of the evolution in the digitalization of critical infrastructure is aptly illustrated by the rolling-out of 5G network technologies, which are considered to have wide and systemic effects on the operation of various critical services and also on business opportunities and economic competition.\footnote{I Stellios and others, ‘A Survey of Iot-enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services’ (2018) 20 IEEE Communications Surveys & Tutorials 3453.} The EU, for instance, views the cybersecurity of 5G networks as ‘an issue of strategic importance’ due to its ‘interconnected and transnational nature’ as infrastructure ‘underpinning the digital ecosystem’,\footnote{E Bertino, SR Hussain and O Chowdhury, ‘5G Security and Privacy: A Research Roadmap’ [2020] arXiv preprint arXiv:2003.13604 <https://arxiv.org/abs/2003.13604> accessed 1 October 2020; D Higgins, ‘Innovation and Risk Walk Hand-in-Hand with 5G and IoT’ (2020) 2020 Network Security 16.} whereas the US policy strives to mitigate the risks to ‘economic and national security from the use of 5G’.\footnote{Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (2019) OJ L88, 42-47.} In sum, the protection of critical digital infrastructure has emerged at the front and centre of many contemporary security discourses. At the same time, however, the security dimensions of critical digital infrastructure extend well beyond traditional ‘hard’ threats, such as terrorist attacks or cyberwarfare, and increasingly touch upon issues such as societal resilience, national competitiveness and technological supremacy.\footnote{White House, ‘National Strategy to Secure 5G of the United States of America’ (2020) <https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf> accessed 1 October 2020.}

**Digital critical infrastructure: evolution of EU law and policy**

The growing significance of critical digital infrastructure is a clear indication of a digital shift in the broader security paradigm. The development and operationalization of the concept have, however, been slow. In order to trace the gradual penetration of critical digital infrastructures into the security discourse, we mapped 40 EU law and policy instruments. Even though the trajectories of digitalization of the society, economy and industry have been identified at least since the 1990s, dedicated legal or policy responses aiming to address and systematize measures that seek to secure critical digital infrastructures only started to emerge from the mid-2000s onwards. The aggregate results of the mapping exercise are collected in Table 1.

As the findings indicate, references to critical digital infrastructures remained diffuse for over a decade, between 2005 and 2015. This stands in sharp contrast with the protection of physical critical infrastructure, which had already become a staple in EU’s security law and policy instruments by 2005.\footnote{Pursiainen (n 19); A Lazari, European Critical Infrastructure Protection (Springer 2014).} References to other digital security threats were similarly mainstreamed in various instruments before the focus on critical digital infrastructures started to mount. Overall, the protection of critical digital infrastructures became a core concern in the EU only after 2017. Since then, however, the concept has been fully embedded in a range of the EU’s core law and policy documents.

Substantively, the analysed instruments follow a similar pattern of gradual evolution. The protection of critical infrastructure appeared on the EU’s regulatory agenda with the 2004 Communication on Critical Infrastructure Protection in the fight against terrorism, which embedded critical infrastructures in a traditional ‘hard’ security paradigm but also recognized the potential impacts of cyber-attacks.\footnote{Commission Communication, ‘A European Programme for Critical Infrastructure Protection’ COM (2006) 786 final.} The following instrument, the 2006 Communication on Critical Infrastructure Protection, refrained, however, from any discussion of the digital dimensions of infrastructure protection.\footnote{AS Campion, ‘From CNOOC to Huawei: Securitization, the China Threat, and Critical Infrastructure’ (2020) 28 Asian Journal of Political Science 47.} This approach was institutionalized in Directive
Table 1. The evolution of EU law and policy

| Year | EU Legal or Policy Instrument | Virtual/digital infrastructures | Positive potential of data-driven technologies | Security implications of data-driven technologies | Physical infrastructures |
|------|--------------------------------|---------------------------------|-----------------------------------------------|-----------------------------------------------|------------------------|
| 2005 | Security of Electricity Supply Directive |                  |                                           |                                               |                        |
| 2006 | Communication on Critical Infrastructures |                  |                                           |                                               |                        |
| 2007 | Critical Infrastructures Directive |                  |                                           |                                               |                        |
| 2008 | Electricity Directive |                  |                                           |                                               |                        |
| 2009 | Natural Gas Directive |                  |                                           |                                               |                        |
|       | Renewable Energy Directive |                  |                                           |                                               |                        |
|       | Regulation on Electricity Networks |                  |                                           |                                               |                        |
|       | Regulation on natural gas transmission networks |                  |                                           |                                               |                        |
| 2010 | Energy Strategy |                  |                                           |                                               |                        |
| 2011 | A Digital Agenda for Europe |                  |                                           |                                               |                        |
| 2012 | Energy Roadmap |                  |                                           |                                               |                        |
| 2013 | Energy Efficiency Directive |                  |                                           |                                               |                        |
| 2014 | Cybersecurity Strategy of the EU |                  |                                           |                                               |                        |
| 2015 | Energy Security Strategy |                  |                                           |                                               |                        |
|       | A policy framework for climate and energy |                  |                                           |                                               |                        |
| 2016 | Digital Single Market Strategy |                  |                                           |                                               |                        |
|       | Integrated Strategic Energy Technology |                  |                                           |                                               |                        |
|       | Energy Union Strategy |                  |                                           |                                               |                        |
| 2017 | Clean Energy for All Communication |                  |                                           |                                               |                        |
|       | General Data Protection Regulation |                  |                                           |                                               |                        |
|       | NIS Directive |                  |                                           |                                               |                        |
| 2018 | Security of Natural Gas Supply Regulation |                  |                                           |                                               |                        |
|       | Building strong cybersecurity for the EU |                  |                                           |                                               |                        |
| 2019 | Artificial Intelligence for Europe |                  |                                           |                                               |                        |
|       | Renewable Energy Directive |                  |                                           |                                               |                        |
|       | Energy Efficiency of Buildings Directive |                  |                                           |                                               |                        |
|       | Regulation on non-personal data |                  |                                           |                                               |                        |
| 2020 | Cybersecurity in the energy sector |                  |                                           |                                               |                        |
|       | Green Deal |                  |                                           |                                               |                        |
|       | EU-China Strategic Outlook |                  |                                           |                                               |                        |
|       | Cybersecurity of 5G networks |                  |                                           |                                               |                        |
|       | Cybersecurity Act |                  |                                           |                                               |                        |
|       | Risk-Preparedness Regulation |                  |                                           |                                               |                        |
|       | Digital Single Market Directive |                  |                                           |                                               |                        |
|       | Security of Electricity Supply Regulation |                  |                                           |                                               |                        |
|       | FDI Regulation |                  |                                           |                                               |                        |
| 2021 | Industrial Strategy |                  |                                           |                                               |                        |
|       | Europe's digital future |                  |                                           |                                               |                        |
|       | European Strategy for Data |                  |                                           |                                               |                        |
|       | Secure 5G deployment |                  |                                           |                                               |                        |
2008/114/EC (the ‘Critical Infrastructures Directive’), a legal instrument whose ambit was limited to energy and transport infrastructures and contained no references to digital threats. While the dedicated security policy instruments refrained from analysing digital security concerns until the 2013 Cybersecurity Strategy of the European Union, other cross-sectoral policy documents registered the impending change. The 2010 A Digital Agenda for Europe, for instance, emphasized the importance of critical information infrastructure and ICT infrastructure, while the 2015 Digital Single Market Strategy addressed privacy and security concerns by referring to ‘secure and trustworthy infrastructures’. In general, however, the policy instruments emphasized the potential of digital technologies instead of their security implications until 2017, when they started to regularly tackle the data, personal and systemic security issues related to the rise of digital technologies. This process has culminated in the work of the von Der Leyen Commission, which has taken a robust stance on various digital threats and also adopted the protection of critical digital infrastructure across its flagship policy instruments, thus setting the tone for the EU’s security, industry, commerce and foreign policies for the coming years.

Even though the need to protect the EU’s digital security has become more widely recognized across different policy sectors, the EU’s legislative competence and its regulatory capacity to achieve such protection are limited. This is due not only to constitutional limitations but also to the fast-paced nature of technological developments, major changes in the security landscape and the EU’s own complex institutional structure. Accordingly, the growing policy relevance of the protection of critical digital infrastructure notwithstanding, the EU legislation contains only a few direct references to the concept. It first appeared on the EU’s legislative agenda with Directive (EU) 2016/1148 (the ‘NIS Directive’), which addresses network and information systems (NIS) and takes a cross-sectoral perspective on the protection of ICT while containing extensive provisions on cybersecurity and infrastructure. Since then, critical digital infrastructure has surfaced in a variety of EU directives and regulations, including Directive (EU) 2018/844 on the energy efficiency of buildings, Regulation 2019/881 (the ‘Cyber Security Act’) and Regulation (EU) 2019/452 (the ‘FDI Regulation’) on the screening of foreign direct investments. To date, the most focused individual instrument tackling the protection of critical digital infrastructure deals with the security of 5G networks but, following evaluation of the Critical Infrastructures Directive, it is likely that the digitalization of security paradigm will feature even more prominently in the EU’s future legislative actions. The FDI Regulation is instructive in this regard, as it casts the protection of the Member States’ virtual critical infrastructure as being part and parcel of the EU’s common commercial policy, thus expanding the focus on critical digital infrastructure beyond cybersecurity to the ownership and control of such infrastructure. While it has been a slow process, the EU’s legal instruments are thus starting to reflect the penetration of critical digital infrastructure both within and beyond security legislation.

31 Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (2008) OJ L345, 75–82.
32 Commission Communication, ‘A Digital Agenda for Europe’ COM (2010) 245 final.
33 Commission Communication, ‘A Digital Single Market Strategy for Europe’ COM (2015) 192 final.
34 K Lenaerts and JA Gutiérrez-Fons, ‘The Constitutional Allocation of Powers and General Principles of EU Law’ (2010) 47 CMLR 1629.
35 Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (2016) OJ L194, 1–30.
36 Directive (EU) 2018/844 amending Directive 2010/31/EU on the energy performance of buildings and Directive 2012/27/EU on energy efficiency (2018) OJ L156, 75–91.
37 Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (2019) OJ L151, 15-69.
38 Regulation (EU) 2019/452 establishing a framework for the screening of foreign direct investments into the Union (2019) OJ L79I, 1–14.
39 Commission Recommendation (EU) 2019/534 (n 25); Commission Communication, ‘Secure 5G Deployment in the EU -Implementing the EU Toolbox’ COM (2020) 50 final.
40 Commission Staff Working Document Evaluation of Council Directive 2008/114 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection, SWD (2019) 308 final.
41 L Reins, ‘The European Union’s Framework for FDI Screening: Towards an Ever More Growing Competence over Energy Policy?’ (2019) 128 Energy Policy 665; Rajavuori and Huhta (n 9).
Even though the EU’s stance on the protection of critical digital infrastructure has become more firmly established over the years, there is still no broadly agreed definition of the concept. Recent uses of the term critical digital infrastructure show it to be a broad concept and the ways in which it is discussed vary. The recent FDI Regulation, for example, lists critical infrastructure, ‘whether physical or virtual’ as a sector in which the Member States are advised to monitor, and potentially prohibit, cross-border investments on the public security grounds.\textsuperscript{42} While the FDI Regulation identifies concrete sectors and industries where the effects of digitalization are easily detected, such as energy, recent policy documents (e.g. the New Industrial Strategy for Europe), use the term more expansively to emphasize the industrial potential and capacity of critical digital infrastructure.\textsuperscript{43} At the same time, the Industrial Strategy also refers to ‘strategic digital infrastructures’, particularly in connection with 5G networks and the forthcoming ‘critical Quantum Communication Infrastructure’.\textsuperscript{44} Regardless of such conceptual variance, however, the EU’s approach to critical digital infrastructure seems to converge under a broad definition that covers physical–digital platforms, systems and networks critical to the functioning of an interconnected and data-driven society.

Judged as a whole, the EU’s policy and legislative initiatives concerning critical digital infrastructure are maturing fast. Analysis of the instruments reveals key patterns with regard to the protection of critical digital infrastructure. The first pattern is temporal, as various digital security concerns seem to have made their appearance on the EU policymakers’ agenda in greater detail only after 2015. The second pattern engages with the institutional integration of the protection of critical digital infrastructures. Due to the relatively minor weight given to digital concerns in the EU’s policy instruments prior to 2016, the digital dimensions of securing key infrastructure have mostly been tackled through policies that seek to leverage the EU’s digital transformation more generally. However, over the past five years or so, the need to protect critical digital infrastructure has begun to inform both the EU’s approach to its external relations and its legislative efforts. In this context, instruments such as the FDI Regulation and recent policies aimed at unlocking the EU’s innovation and industrial potential amidst great power competition embed the protection of critical digital infrastructure more fully in the broader trajectories of the digitalization of security, and this approach extends to issues relating to the ownership of technology and data.

3. GOVERNING DIGITAL SECURITY: THE PROTECTION OF CRITICAL DIGITAL INFRASTRUCTURE IN THE EU’S ENERGY SECTOR

The effects of digitalization and data-driven technologies on the energy sector

The trends and phenomena identified above are highly relevant to the energy sector. Like other industries, energy systems are undergoing a fundamental digital transformation. The growing significance of data-driven solutions in the energy sector, which is moving towards a low-carbon model, can clearly be seen in respect of issues such as the high share of variable distributed renewable energy, more flexible demand, energy efficiency, energy storage facilities and sector coupling.\textsuperscript{45} The connection between data and energy is most acutely reflected in the efforts being made to integrate the increasing share of renewable energy sources into the generation mix and to increase the market flexibility that will inevitably be needed to achieve such integration.\textsuperscript{46}

\textsuperscript{42} The FDI Regulation (n 38) 1–14.
\textsuperscript{43} Commission Communication, ‘A New Industrial Strategy for Europe’ COM (2020) 102 final.
\textsuperscript{44} \textit{ibid.}
\textsuperscript{45} G Erbach and J O’Shea, ‘Cybersecurity of Critical Energy Infrastructure’ (\textit{European Parliament Briefing}, 2019) \texttt{<https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642274/EPRS_BRI(2019)642274_EN.pdf>} accessed 1 October 2020.
\textsuperscript{46} A Vernotte and others, ‘Load Balancing of Renewable Energy: A Cyber Security Analysis’ (2018) 1 Energy Informatics 5; S Kloppenburg and M Boekelo, ‘Digital Platforms and the Future of Energy Provisioning: Promises and Perils for the next Phase of the Energy Transition’ (2019) 49 Energy Research & Social Science 68.
Examples abound. Artificial intelligence (AI) applications, for instance, can be used to integrate the increasing shares of renewable energy into the energy mix, to facilitate the electrification of transportation by automating not just the driving of individual vehicles but the operation of entire traffic systems and to improve the energy efficiency of buildings. The Internet of Things (IoT) can be used to optimize entire industrial supply chains and to manage the energy production and consumption of smart cities. The operation of batteries, which increases the flexibility of the electricity system, increasingly relies on access to and utilization of large datasets to identify and address the points at which balancing measures are needed. For instance, vehicle-to-grid technology, where the combined and optimally charged fleet of electric vehicles is used as a battery for peak-load reduction and load balancing depends extensively on data and analytics to forecast and steer the system needs. Similarly, smart-grid development overall is predicated on the assumption that the management functions of electricity transmission and distribution can be automated and steered digitally. The ‘smartening’ of the energy sector is reflected not only in the production and transportation of energy but also in the homes of final consumers, where internet-connected smart appliances, smart homes and smart meters take care of many of the things previously handled by means of manual labour. Digital energy platforms can be used to optimize the planning and utilization of decentralized energy systems by managing connections between households, steering energy flows depending on consumption needs and identifying further investment needs for a specific area.

The growing emphasis on data-driven solutions in the energy sector has wide-ranging security implications. In addition to the cybersecurity of energy systems, questions of data protection and privacy have emerged as part of the evolving security paradigm in the energy sector, as the data that are being used to fuel the new technologies can ultimately be traced back to an individual person’s actions in everyday life. For example, using electric vehicles as a battery to balance the electric system involves the collection of user data, such as location, driving routes or parking routines. Such information can reveal much about a person’s private life and can be used, for instance, to deduce when a person’s home is unoccupied for longer periods of time. In addition to the apparent exposure to external threats such as cyber-attacks and malicious hackers, the data-driven technologies face internal risks, such as poor design, inadequate implementation or deficient configuration, which may impact the security of the energy system. Smart grids, for example, can encounter multiple technical and non-technical threats such as infrastructural security, technical operational security, the systems’ data management security as well as non-technical threats posed by poor environmental security and governmental intervention. Moreover, the interconnectedness of these, typically Internet-based, technologies deepens the potential effects of any disturbance. A network of mutually interconnected digital technologies governing different functions in the energy value chain exposes the energy sector to incidents that have more far-reaching effects than would be the case in a more isolated, closed system.

The particularities that necessitate a specialized sectoral approach to energy include, for example, the real-time requirements of balancing electricity systems, which make reaction times to security threats remarkably short. The energy system is also typically a combination of advanced and legacy technologies installed decades ago. The cross-functionality of these technologies creates another layer of complexity in relation to

47 M Masikos and others, ‘Machine-Learning Methodology for Energy Efficient Routing’ (2013) 8 IET Intelligent Transport Systems 255.
48 AI Dounis, ‘Artificial Intelligence for Energy Conservation in Buildings’ (2010) 4 Advances in Building Energy Research 267.
49 G Bedi and others, ‘Review of Internet of Things (IoT) in Electric Power and Energy Systems’ (2018) 5 IEEE Internet of Things Journal 847.
50 H Fathabadi, ‘Novel Grid-Connected Solar/Wind Powered Electric Vehicle Charging Station with Vehicle-to-Grid Technology’ (2017) 132 Energy 1.
51 L Edwards, ‘Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective’ (2016) 2 European Data Protection Law Review 28.
52 Erbach and O’Shea (n 45).
53 AO Otuozo, MW Mustafa and R Masood Larik, ‘Smart Grids Security Challenges: Classification by Sources of Threats’ (2018) 5 Journal of Electrical Systems and Information Technology 468.
54 Kiravuo and others (n 13).
55 Erbach and O’Shea (n 45).
addressing security issues in the digital context. The inherent interconnectedness of energy supply chains, particularly electricity systems, makes them especially vulnerable to the far-reaching effects even of small incidents. These specificities are most recently reflected in the Clean Energy for All Europeans package, which includes legal instruments that allow for the adoption of technical rules that address cybersecurity aspects of cross-border electricity flows.

All data-driven technologies run on electricity, which makes them entirely dependent on energy supply irrespective of the sector examined. Increasing societal reliance on new technologies underlines the importance of energy security, ie the uninterrupted availability of affordable energy. Accordingly, data-driven technologies are entirely dependent on energy, and vice versa. This interdependence has two key consequences. First, it increases the importance of safeguarding energy security. Secondly, the legal and policy solutions taken to address data-driven technologies increasingly pervade the energy sector, and vice versa.

Furthermore, the potential effects of the interconnectedness between energy security and data-driven technologies are likely to increase rather than decrease in the years to come. For example, sector coupling entails linking and finding synergies between sectors in the interests of energy efficiency and decarbonization. These interdependencies between sectors, combined with mutually interconnected data-driven technologies, only increase the importance of ensuring energy security. This inherent interdependence between data-driven technologies and ensuring a continuous energy supply means that the legal and policy solutions taken to pursue energy security also have an impact on the future functioning of data-driven technologies.

The interdependence between energy and data-driven technologies necessitates the broadening of the scope of EU law and policy applicable to the energy sector to cover issues that address critical digital infrastructures in different stages of the life cycle of data-driven technologies. This is also demonstrated by the findings presented in Table 1. For much of the EU’s history, the energy sector has been governed by the politically charged application of Treaty rules and by sector-specific policies and regulations developed since the 1990s. Digitalization challenges this approach. Most of the cross-sectoral legal instruments discussed in this article apply without distinction between different sectors and are, therefore, relevant to the energy sector. The pace of technological change also presents a challenge in terms of the development of legal and policy frameworks capable of coping with the complexity and interdependency of energy and data-driven technologies. For decades, energy was a relatively slow-moving, technologically predictable industry and this was often reflected in the legal and regulatory environment. Today, the rapid changes taking place in the energy transition and the new phase of technology-driven transformation can make it difficult for policymakers to stay ahead of the curve. Some jurisdictions have made progress in addressing these issues, but there is unfinished business everywhere. Major security risks could ensue if regulatory change fails to keep up with the fast pace of technological change.

For all these reasons, today’s energy sector amounts to a highly complex system. In general, the more complex the system, the more difficult it is to address through legal and policy instruments and the more difficult it is to measure security risks and their effects empirically. The same consideration makes it difficult to predict the security risks that will arise with any degree of certainty. In the light of these considerations, it
is no surprise that the legal and policy measures that have been adopted to address new security concerns are highly complex in nature and mirror the complexities involved in the digitalization of the energy sector.

The protection of critical digital infrastructure in the EU’s energy sector

The energy sector has always been at the very core of EU legal and policy measures as two of the three founding treaties were specifically designed to address energy. The EU’s explicit competence to legislate in the sector was, however, left to the Member States until the 2009 Lisbon Treaty. Until then, energy was mainly addressed under common rules on the harmonization of laws and through environmental policy. Even after the Treaty of Lisbon, the energy sector has continued to be addressed through various policies and cross-sectoral instruments, including the common commercial policy.

As illustrated in Table 1, the energy sector has also been at the very core of EU legal and policy measures protecting critical infrastructures. The earliest EU legal and policy measures that sought to protect essential technologies and critical infrastructures were limited in scope but explicitly addressed core elements of the energy sector. Since then, it seems the role of the energy sector in protecting essential technologies and critical infrastructures has increased rather than decreased. Depending on the context and discourse, different segments of the energy value chain are considered critical infrastructures. In some contexts, the entire sector can be considered a critical infrastructure.

The 2005–10 EU legal and policy approaches focused solely on protecting physical energy assets from physical attack or extreme weather conditions. While such instruments were to be found in the sector-specific energy legislation, the first cross-sectoral instruments, including Directive 2008/114/EC (the ‘Critical Infrastructures Directive’), were specifically applicable to the energy sector. Since these earlier legal and policy initiatives, the role of data and data-driven technologies and the potential security concerns they pose for the energy sector have increased in both sector-specific and cross-sectoral legal and policy instruments.

As was the case with the EU’s cross-sectoral policy instruments, most of the pre-2015 energy-specific legal and policy instruments focused on the positive potential of data-driven technologies in achieving the low-carbon transition. The 2010 Energy Strategy for 2020 even argued that without a technological shift, ‘the EU will fail on its 2050 ambitions to decarbonise the electricity and transport sectors’. Such claims were made in the context of a broader technological shift in the EU and concerns over fierce competition in international technology markets. Unlike these energy-specific legal instruments, the cross-sectoral policy documents highlighted some privacy and security concerns in the context of digitalizing critical infrastructures. Despite the lack of reference to the novel digital security issues in the energy-specific instruments, some of these general concerns were translated into legal obligations in EU energy law for the first time in 2012.

---

64 Treaty establishing the European Coal and Steel Community. Paris, 18 April 1951 (ECSC); Treaty establishing the European Atomic Energy Community (Euratom), Rome, 25 March 1957; Snell and Aalto (n 14).
65 Critical Infrastructures Directive (n 31) 75–82.
66 CJK Sandoval, ‘Cybersecurity Paradigm Shift: The Risks of Net Neutrality Repeal to Energy Reliability, Public Safety, and Climate Change Solutions’ (2019) 10 San Diego Journal of Climate and Energy Law 91.
67 CV Mikellidou and others, ‘Energy Critical Infrastructures at Risk from Climate Change: A State of the Art Review’ (2018) 110 Safety Science 110.
68 Directive 2005/89/EC concerning measures to safeguard security of electricity supply and infrastructure investment (2006) OJ L33, 22–27.
69 Commission Communication (n 30); Critical Infrastructures Directive (n 31) 75–82.
70 Directive 2009/28/EC on the promotion of the use of energy from renewable sources and amending and subsequently repealing Directives 2001/77/EC and 2003/30/EC (2009) OJ L140, 16–62; Commission Communication, ‘Energy 2020 A Strategy for Competitive, Sustainable and Secure Energy’ COM (2010) 639 final; Commission Communication, ‘Energy Roadmap 2050’ COM (2011) 885 final; Commission Recommendation (EU) 2019/534 (n 25).
71 Commission Communication, ibid.
72 Commission Communication (n 32).
Thus, Directive 2012/27/EU (the ‘Energy Efficiency Directive’) obliged Member States to ensure ‘the secur-
ity of the smart meters and data communication, and the privacy of final customers, in compliance with rele-
vant Union data protection and privacy legislation’.73 This was six years before the entry into force of
Regulation (EU) 2016/679 (the ‘General Data Protection Regulation’),74 which replaced the much more
narrowly focused Directive 95/46/EC.75

The 2015 Digital Single Market Strategy, which established the EU policy stance on free movement in the
digital era, generated more explicit interlinkages between the cross-sectoral and sector-specific policy initia-
tives. It discussed the security implications of digital services and the handling of personal data in the context
of secure and ‘trustworthy’ infrastructures, while highlighting that digitalization ‘offers unprecedented oppor-
tunities to other economic sectors, such as transport (e.g. intelligent transport systems) or energy (e.g. smart
grids, metering)’.76 In 2016, the Energy Union and Clean Energy for All Europeans initiatives continued in
this vein by emphasizing the positive potential of data-driven technologies to the energy sector while also
linking the potential security implications with the issues previously underlined in the Digital Single Market
Strategy.77 The Energy Union Communication, which laid out the strategic priorities of the EU’s energy pol-
cy, emphasized that the EU would continue to look for synergies between the Digital Single Market Strategy
and energy policy and to push for smart technologies in the energy sector while taking ‘measures to ensure
privacy protection and cyber-security’.78

The first institutionalized policy discussions linking energy, security, critical digital infrastructures and
data-driven technologies took place as late as 2017. Both the positive potential and the security implications
of data-driven technologies for critical digital infrastructure in the energy sector were explicitly recognized, al-
beit in a Parliament briefing, which has little institutional weight in steering EU policy.79 This coincided, how-
ever, with the implementation period of the NIS Directive, which focuses on the protection of ICT
infrastructures and allows sector-specific factors to be taken into account in evaluating the disruptive effect
on essential services, such as energy supply.80

Over the last two years, the security discourse applicable to critical infrastructures and energy has become
fully embedded in the digital sphere. This is reflected not only in the energy-specific legal and policy instru-
ments but also in cross-sectoral instruments. For example, the 2018 Artificial Intelligence for Europe
Communication explicitly highlights not only the relevance of AI to the energy sector but also its role in
improving energy efficiency in all sectors.81 On the legal side, the Clean Energy for All Europeans package
includes several instruments that underscore the importance of digitalization in the context of the energy
transition but also address security and privacy concerns arising from increasing reliance on data-driven tech-
nologies.82 Directive (EU) 2018/2001 (the ‘Renewable Energy Directive’) emphasizes the need for intelli-
gent networks and intelligent transport as well as smart cities and smart communities,83 while Regulation

73 Directive 2012/27/EU on energy efficiency, amending Directives 2009/125/EC and 2010/30/EU and repealing Directives 2004/8/EC
and 2006/32/EC (2012) OJ L315, 1–56.
74 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement
of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) OJ L119, 1–88.
75 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such
data (1995) OJ L281, 31–50.
76 Commission Communication (n 33).
77 Commission Communication, ‘A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy’
COM (2015) 80 final; Commission Communication, ‘Clean Energy For All Europeans’ COM (2016) 860 final.
78 Commission Communication (2015) ibid.
79 Erbach and O’Shea (n 45).
80 NIS Directive (n 35) 1–30.
81 Commission Communication, ‘Artificial Intelligence for Europe’ COM (2018) 237 final.
82 Commission Communication (2016) (n 77).
83 Directive (EU) 2018/2001 on the promotion of the use of energy from renewable sources (2018) OJ L328, 82–209.
The cross-sectoral legal and policy discussion has also recognized the specificities of the energy sector in addressing the new digital security scenery. It has been highlighted that the energy system possesses ‘a number of particularities that necessitate a specialised sectoral approach to cybersecurity, above and beyond cybersecurity standards and measures applied to information technology systems’. These references not only highlight the threats and security concerns posed by data-driven technologies in the energy sector but also underline their importance to the energy transition. For instance, the 2019 Commission Recommendation on the Cybersecurity of 5G Networks, which also discusses fifth-generation networks in the context of critical infrastructures and essential services, contains several references to energy. In particular, the recommendation highlights that, once rolled out, 5G networks will ‘form the backbone for a wide range of services essential for the functioning of the internal market and the maintenance and operation of vital societal and economic functions – such as energy’. Similarly, the 2020 Communication on Europe’s Digital Future emphasizes the need for additional investment in smart energy and transport infrastructures.

Despite the emergence of policy initiatives addressing the evolving security paradigm, the majority of the most recent sector-specific legal and policy measures still heavily emphasize the positive potential of data-driven technologies in addressing issues affecting the transitioning sector. Decarbonization and efficiency gains within the energy sector are the primary touchstones across the relevant EU instruments. Most recently, the importance of data-driven technologies in the energy sector was underlined in the European Green Deal, which promises to ‘explore measures to ensure that digital technologies such as artificial intelligence, 5G, cloud and edge computing and the internet of things can accelerate and maximize the impact of policies to deal with climate change’. Similar trends can be recognized in other cross-sectoral instruments.

On the other hand, legal instruments such as the 2019 FDI Regulation, which establishes a framework for the screening of foreign direct investment on grounds of security or public order, explicitly allow state intervention to limit investment in digital energy infrastructures. Similarly, policy instruments such as the 2020 Industrial Strategy address both the need to facilitate data-driven technologies and the need to protect society from the security implications of their use.

In sum, the most recent legal and policy initiatives stress that the risk scenarios facing critical infrastructures in the EU have evolved to include issues that arise in digitalized and virtual contexts. This evolution highlights the interconnectedness and the associated vulnerabilities of our digital critical infrastructure, especially in the energy sector.

### 4. ANALYSIS AND CONCLUSIONS

This article has analysed the dynamics and implications of the digitalization of security in the energy sector through an evolutionary review of EU legal and policy instruments over the past 15 years and through a doctrinal legal analysis of the applicable legal instruments. Our analysis reveals substantial changes in the

---

84 Regulation (EU) 2019/941 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC (2019) OJ L158, 1–21.
85 Erbach and O’Shea (n 45).
86 Commission Recommendation (EU) 2019/534 (n 25).
87 Commission Communication, ‘Shaping Europe’s Digital Future’ COM (2020) 67 final.
88 Vernotte and others (n 46).
89 Commission Communication, ‘The European Green Deal’ COM (2019) 640 final.
90 Commission Communication (n 87).
91 The FDI Regulation (n 38) 1–14; Rajavuori and Huhta (n 9).
92 Commission Communication (n 43).
93 Commission Staff Working Document Evaluation of Council Directive 2008/114 (n 40).
94 Erbach and O’Shea (n 45).
conceptions and dynamics of security in the energy sector. In particular, we find four broad patterns that characterize the digitalization of security in the energy sector.

First, we note that digitalization has penetrated into the core of the energy sector’s security paradigm only recently. As the evolution of the EU’s law and policy instruments indicates, even the most integrative instruments have embraced the digital risks of the energy transition only in the past few years. This is reflected not only in the substance of EU legal and policy documents but also in terms of the number of references made and documents produced in relation to this area. While the physical security threats to critical energy infrastructures dominated the legal and policy initiatives around 2005–07, the most recent instruments are fully engaged with the protection of virtual or digital critical infrastructures. Substantively, the most recent legal and policy documents portray a significantly more nuanced approach to the various digital threats than those produced prior to 2010.

Secondly, we uncover a significant disconnect in conceptualizing risks and opportunities associated with digitalization. The general trend towards digital risks being ever-present in almost all fields notwithstanding, significant divergences remain across the broader digitalization of security landscape. Accordingly, the EU’s legal ‘hard security’ instruments that focus, for example, on the protection of critical digital energy infrastructure or the input data operate on an entirely different register than most policy instruments that encourage the development of new data-driven technologies, for example, in relation to the low-carbon transition. In a sense, ensuring the security of critical infrastructures falls into the category of traditional, ‘hard’ security thinking and risk aversion, whereas the general policy approach to developing new data-driven technologies aims to be dynamic, fast, forward-looking, innovative and prepared to take risks. In fact, a large proportion of the security discussion in both the legal and policy documents took place after the positive potential of facilitating data-driven technologies had been highlighted. These conflicting approaches have the potential to clash with one another. One requires the facilitation of investment in data-driven technologies and the other requires control over the same investment and the data that are used to fuel the technologies. This conflict makes further evolution of the conventional security paradigm likely.

Thirdly, we identify a move from sectoral regulation of digitalized security in the energy sector to a distinctly cross-sectoral approach. In the EU context, this is illustrated by the encroachment of broadly applicable regulations and directives on different parts of the energy value chain, suggesting that the EU’s broader law and policy changes increasingly affect the security of the energy sector. Even the earliest cross-sectoral legal instruments addressing the security of solely physical infrastructures applied to energy. However, the ever-growing cross-sectoral focus on the security implications of data-driven technologies increasingly pervades the legal and policy framework governing the energy sector. This means that thinking about security in sectoral silos is no longer possible given the interconnectedness of data-driven technologies. The growing and cross-cutting focus on critical digital infrastructure illustrates this change.

Finally, we note that the concept of energy security does not feature in the overall security discourse relating to the use of data-driven technologies in the energy sector. This is despite the fact that all data-driven technologies run on electricity, which makes these technologies entirely dependent on energy supply irrespective of the sector examined. This is a crucial omission considering the reliance of data-driven technologies on the secure supply of energy, and we suggest that the concepts of energy security and digitalization of security need to be reconciled more fully in the future.

Collectively, our findings illustrate a rapid evolution of digitalization of security in the energy sector and beyond. While they remain conceptually elusive, digital risks increasingly frame the overall security conceptions across policy fields ranging from the cybersecurity of energy systems to privacy in smart systems and strategic technological competition. Further multidisciplinary research is required to fully appreciate the difficulties that legislators, policymakers, managers and researchers face when trying to keep up with the rapid

95 C Strambo, M Nilsson and A Månsson, ‘Coherent or Inconsistent? Assessing Energy Security and Climate Policy Interaction within the European Union’ (2015) 8 Energy Research & Social Science 1.
technological change in the energy transition and the ensuing evolution of the energy sector’s security paradigm.

ACKNOWLEDGEMENTS
This work was supported by the Academy of Finland [grant number 324037].

DECLARATION OF COMPETING INTEREST
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.