German Law Journal (2020), **21**, pp. 1149–1179
doi:10.1017/glj.2020.67

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective

Christian Calliess* and Ansgar Baumgarten**

(Accepted 10 March 2020)

Abstract
Cybersecurity in the financial sector is a dynamic and evolving policy field with unique challenges and specific characteristics. While it has recently received a lot of attention from disciplines like Economics and Politics, legal literature on this topic, especially with regard to EU law, still lags behind. This is surprising, given that cybersecurity in the EU is characterized by complex governance structures, a variety of legal sources, and a wide range of different rule makers and involved actors, and given that only a clear legal framework with efficient institutions at both EU and Member State level can provide for a safe digital environment. The purpose of this Article, therefore, is twofold: On the one hand, it aims to introduce the legal aspects of cybersecurity in the financial sector while taking stock of existing cybersecurity schemes, including their strengths and weaknesses from a legal perspective. On the other hand, it will set out key elements that cybersecurity regulation in the financial sector must respect in order to be effective and come up with reform proposals to make the EU financial sector more cybersecure.

Keywords: Cybersecurity; financial sector; European Union; standard setting; European cybersecurity platform

A. Introduction

The spokesperson of an influential hackers club once compared the world's digital infrastructure to a poorly maintained system of water pipes in a developing country megalopolis. Leaks can be found in every nook and corner; technicians try to plug the holes 24/7; but all they have is duct tape.[1]

Alongside space, air, land, and sea, cyber is the fifth dimension. It opens a global virtual world, radically changing societies and shaking classical borders. But a digital world also comes with new types of micro threats on businesses and citizens, and macro threats on public policies and state security, which are asymmetrical, unpredictable, and unaffected by classical state responses. They occur at

*Prof. Dr. Christian Calliess is a Professor for Public and European Law at Freie Universität Berlin, Germany and holder of an Ad Personam Jean-Monnet-Chair. Dr. Calliess studied law at the Universities of Saarbrücken and Göttingen. Dr. Calliess later received a Master in Advanced European Studies at the College of Europe in Bruges and a PhD at the University of Saarbrücken. From 2015–18 he was on leave from his chair in order to work as Legal Adviser to the European Political Strategy Center (EPSC), the in-house think tank of the European Commission, working under the authority of its President Jean-Claude Juncker and advising him.

**Ansgar Baumgarten is a PhD candidate and scientific assistant for Dr. Calliess at Freie Universität Berlin. Baumgarten studied law at Humboldt Universität zu Berlin and later received his Maîtrise en droit from l'Université Paris II and his LL.M. from King's College London.

This Article has been prepared by the authors as an independent academic work under the 2019 Legal Research Programme sponsored by the ECB. Any views expressed are only those of the authors and do not necessarily represent the views of the ECB or the Eurosystem. The Article has benefited from the exchange of ideas with Prof. Dr. Chiara Zilioli, Marcin Opoka, and Emran Islam and helpful discussions with the ECB's Legal Services team.

[1]Frank Rieger, *Jeder ist angreifbar*, DER SPIEGEL, Sept. 19, 2015, at 68.

© The Author(s), 2020. Published by Cambridge University Press on behalf of the *German Law Journal*. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

the level of tricksters and range up to state espionage and, potentially, offensive cyber-attacks against states. Cyber is as such a new global world, where there is no dividing line between external and internal security. There is an attacker in one country, aiming for a target in another, causing damage in yet a third. There are as well large-scale attacks targeting and affecting several Member States at once—with the actual attack being carried out in cyberspace, which does not even adhere to one spot, country, or continent, but is a dimension for itself. This raises the question of the adequacy, or inadequacy, of the classical regulatory tools to reply to these challenges.[2]

In this new environment, the EU and its Member States need to anticipate and plan for hitherto unimaginable scenarios in which they would be put if under a severe cyber-attack. This is particularly true for the implementation of the European Commission's EU Digital Single Market agenda.[3] With the financial industry at its very center, a digital single market for the free movement of persons, services, and capital is highly dependent on a reliable and robust IT infrastructure. Comparable to the field of "industry 4.0," innovation in the financial sector—for example, the idea of a "Digital City," a financial platform of Europe that coordinates a network of financial centers in the EU[4]—and the success of new business models depend on trust in a safe digital environment.

Cybersecurity is a term that covers a wide range of activities. Broadly speaking, it can be divided into three different categories: Network and information security, fight against cybercrime, and cyber defense. With regard to network and information security, cybersecurity can be defined as the ability of network and information systems to resist action that compromises the availability, authenticity, integrity, or confidentiality of digital data or the services those systems provide.[5] This Article will focus on cybersecurity in the financial sector in its dimension of network and information security. Still, it will also refer to the other two areas of cybersecurity where necessary and appropriate. The financial sector is understood as the entirety of payment systems, credit institutions, payment institutions, stock exchanges, trade repositories, central securities depositories, central counterparty clearing houses, securities settlement platforms, credit rating agencies, insurance companies, and asset management companies.

The disruptive effects of a successful cyber-attack against the financial sector can be devastating, resulting in financial shocks. In November 2018, Benoît Cœuré, member of the Executive Board of the European Central Bank (ECB), pointed out, "the next financial crisis may well start as a cyber-incident."[6] In March 2017, the G20 Finance Ministers and Central Bank Governors noted, "the malicious use of information and communication technologies could disrupt financial services crucial to both national and international financial systems, undermine security and confidence, and endanger financial stability."[7] A breakdown of wholesale payment systems can endanger the provision of liquidity by central banks and jeopardize the implementation of

[2]*See generally* Nathan A. Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503 (2013).

[3]*See generally* Darko Samardžić & Tobias Fischer, *European Integration from a Single to a Digital Single Market*, 21 ZEITSCHRIFT FÜR EUROPARECHTLICHE STUDIEN 329 (2018).

[4]Joachim Wuermeling, *Vernetzte Finanzzentren*, HANDELSBLATT, Mar. 02, 2018, at 72.

[5]*See* Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016, art. 4(2), 2016 O.J. (L194) 1 [hereinafter NIS Directive] (concerning measures for a high common level of security of network and information systems across the Union). For a comprehensive discussion of the term "cybersecurity law" see Jeff Kosseff, *Defining Cybersecurity Law*, 103 Iowa L. Rev. 985 (2018).

[6]Benoît Cœuré, *The new frontier of payments and market infrastructure: on cryptos, cyber and CCPs*, EUROPEAN CENTRAL BANK, (Nov. 15, 2018), https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp181115.en.html (welcome remarks at the Economics of Payments IX conference).

[7]Press Release, G20 Germany 2017, G20 Finance Ministers and Central Bank Governors Meeting (Mar. 18, 2017), http://www.g20.utoronto.ca/2017/170318-finance-en.pdf. For a comprehensive analysis of cyber risks as threats to financial stability, see MARTIN BOER & JAIME VAZQUEZ, CYBER SECURITY & FINANCIAL STABILITY: HOW CYBER-ATTACKS COULD MATERIALLY IMPACT THE GLOBAL FINANCIAL SYSTEM (Institute of International Finance, 2017), https://www.iif.com/Portals/0/Files/IIF%20Cyber%20Financial%20Stability%20Paper%20Final%2009%2007%202017.pdf?ver=2019-02-19-150125-767; Jason Healey, Patricia Mosser, Katheryn Rosen & Adriana Tache, *The future of financial stability and cyber risk*, BROOKINGS CYBERSECURITY PROJECT (2018), https://www.brookings.edu/research/the-future-of-financial-stability-and-cyber-risk/.

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

monetary policy.[8] At the micro-level, a successful cyber-attack may result in the theft or loss of funds and intellectual property, the manipulation or loss of sensitive corporate or customer information, and the interruption of services provided by a financial institution. A successful cyber-attack can also cause indirect costs such as negative effects on customer relationships, diminished reputation, and, potentially, regulatory sanctions and civil liability.[9]

It, therefore, comes as no surprise that cybersecurity has attracted a lot of attention from national, European, and international policy makers in recent years, especially with regard to the financial sector. Subsequently, a complex picture of different actors, bodies, and regulatory schemes has emerged. Likewise, the private sector reinforced its efforts to build up stronger cybersecurity capabilities.

This Article proceeds in five parts. It aims to provide a comprehensive analysis of the current EU regulatory environment for cybersecurity in the financial sector, and to identify its strengths and weaknesses from a legal perspective—a topic that has not yet received a lot of attention in legal literature. Following a brief overview of the current cyber threat landscape in Section B, the Article develops a framework of key elements that cybersecurity regulation in the financial sector must respect in order to be effective and clarifies the role of the private sector and public authorities in protecting the financial sector against cyber-attacks in Section C. Subsequently, the Article provides a stock take of the current legal framework for cybersecurity in the financial sector. While Section D focuses on the overall legal framework for cybersecurity in the financial sector, Section E examines the legal situation at the EU level in more detail. In this regard, EU cybersecurity schemes for systemically important payment systems and credit institutions are used as reference areas. Finally, the Article explores possible ways forward to make the EU financial sector more cybersecure. In this regard, only a clear legal framework with efficient institutions at both EU and Member State level can provide for a safe digital environment, as considered in Section F.

B. Overview of the Threat Landscape

I. Categories of Cyber Threats

In recent years, cyber-attacks have grown rapidly in scale, scope, and sophistication.[10] They concern the entire ecosystem, whether states, individuals, or businesses, and question a number of important dichotomies, including internal/external, public/private, and civilian/military.[11] Cyber-attacks are part of "hybrid-threats," a "mixture of conventional and unconventional, military and non-military, overt and covert actions that can be used in a coordinated manner by state or non-state actors to achieve specific objectives."[12] They can be attributed to four different and, to some extent, overlapping threat-categories.

[8]Benoît Cœuré, *The Future of Financial Market Infrastructures: Spearheading Progress Without Renouncing Safety*, European Central Bank, (June 26, 2018), https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180626.en.html (Speech at the Central Bank Payments Conference). For more details on liquidity risks caused by cyber shocks, see Emanuel Kopp, Lincoln Kaffenberger & Christopher Wilson, *Cyber Risk, Market Failures, and Financial Stability* 21–22 (International Monetary Fund, Working Paper No. 17/185, 2017).

[9]Kopp, Kaffenberger & Wilson, *supra* note 8, at 9–11; Barry Connolly, *Cybersecurity Breaches: The Risks and How to Mitigate Them*, https://fod.ie/wp-content/uploads/2017/03/Cybersecurity-breaches-the-risks-and-how-to-mitigate-them.pdf. For a comprehensive overview of the consequences of a successful cyber-attack, see Tom Webley & Peter Hardy, *What Can Be Done to Mitigate Cyber Risk?*, 6 J. Int'l Banking & Fin. L. 353, 354 (2015).

[10]Cœuré, *supra* note 6.

[11]Helena Carrapico & André Barrinha, *The EU as a Coherent (Cyber)Security Actor?*, 55 J. Common Mkt. Stud. 1254, 1255 (2017). *See generally* Elaine Fahey, *The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security*, 5 Eur. J. Risk Reg. 46 (2014).

[12]European Commission Press Release IP/16/1227, FAQ: Joint Framework on Countering Hybrid Threats (Apr. 6, 2016), http://europa.eu/rapid/press-release_MEMO-16-1250_en.htm.

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

1. Cyber War

Cyber war, or hybrid forms of it, is usually a state-sponsored form of action against another state carried out via electronic networks. It includes warfare against another state's military, public, and private sectors, as well as the civilian population. Until now below the threshold of formally declared warfare, cyber aggressions are likely to be used with greater intensity and accuracy in the future, opening the door for "think the unthinkable" types of scenarios in the years to come. Due to the anonymity of the internet, the attribution of cyber-attacks is complicated, and perpetrators often remain unidentified. Typical tools of cyber war include botnets and worms such as Stuxnet, a computer worm first discovered in July 2010, and deemed a joint Israeli/US effort to disrupt Iran's nuclear program.[13] A less intrusive, but just as dangerously efficient, way of harming other states and players is electronic disinformation and propaganda. Yet, what is new is the increasingly systematic use of cyberspace by states to pursue national foreign and security policy objectives. Cyber-attacks are getting more sophisticated and more aggressive, targeting critical infrastructures to potentially disrupt states.

2. Cyber Espionage

Cyber espionage concerns breaches in the databases of public authorities and state or non-state enterprises by foreign governments to gather information such as trade secrets and strategically important corporate knowledge. In December 2018, the US and the UK accused hackers linked to the Chinese Ministry of State Security of obtaining unauthorized access to the computers of at least forty-five entities, including commercial and defense technology companies and US government agencies such as NASA and the US Navy.[14]

3. Cyber Terrorism and Cyber Vandalism

Cyberterrorism is the use of cyberspace to commit terrorist acts such as hacking into a system to cause a nuclear plant to melt.[15] Below the threshold of cyber terrorism, cyber vandalism has no specific objective or target. It is carried out "more for the thrill than anything else."[16]

4. Cybercrime

Cybercrime, such as phishing,[17] online fraud, and online forgery, involves offenses against property rights, including intellectual property, launched by non-state actors. It is a threat to everybody. "Cybercrime as a service" is becoming a widely used practice. Facilitated by the dark net, hacking can be ordered and purchased as easily as a taxi. Cybercrime is growing very fast and has dramatic economic costs. As a percentage of global GDP, cybercrime cost the global economy 0.8 percent of GDP in 2016, up from 0.62 percent in 2014.[18] Globally, it will cost businesses over five trillion US dollars per year by 2024.[19] Cyber-attacks can massively affect the business community.

[13]Annegret Bendiek & Andrew Porter, *European Cyber Security Policy Within a Global Multistakeholder Structure*, 18 Eur. Foreign Aff. Rev. 155, 162 (2013); *see also* Ellen Nakashima & Joby Warrick, *Stuxnet Was Work of U.S. and Israeli Experts, Officials Say*, Wash. Post (June 2, 2012), https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

[14]Patrick Wintour, *US and UK accuse China of sustained hacking campaign*, Guardian (Dec. 21, 2018), https://www.theguardian.com/world/2018/dec/20/us-and-uk-accuse-china-of-sustained-hacking-campaign.

[15]Bendiek & Porter, *supra* note 13, at 158.

[16]*Id.*

[17]Bendiek & Porter, *supra* note 13, at 159 (noting that the term "phishing" refers to the fraudulent acquisition of sensitive information using electronic communications, whereby perpetrators impersonate trusted people).

[18]James A. Lewis, Economic Impact of Cybercrime—No Slowing Down 6 (2018), https://assets.website-files.com/5bd672d1924b9893a632c807/5c171d5e85ed62697a79e351_economic-impact-cybercrime.pdf.

[19]Press Release, *Business Losses to Cybercrime Data Breaches to Exceed $5 trillion by 2024*, Juniper Research (Aug. 27, 2019), https://www.juniperresearch.com/press/press-releases/business-losses-cybercrime-data-breaches.

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

The most affected sectors are banking and utilities—with 18.37 and 17.84 million US dollars on average annual cost of cybercrime for each organization in the industry in 2018.[20] Cyber-attacks can also ruin the reputation of companies building their business model on private data or, like financial institutions, on confidence and trust.

The financial sector is of particular attractiveness for cyber criminals seeking illicit financial gains.[21] In 2016, customers of financial services suffered sixty-five percent more cyber-attacks than customers of any other industry.[22] In July 2014, JP Morgan Chase was the victim of a hack that comprised the accounts of seventy-six million households and seven million small businesses.[23] In February 2016, eighty-one million dollars were stolen from an account of the central bank of Bangladesh via the SWIFT network.[24] In November 2016, around 2.5 million pounds were stolen from around 9000 customers of Tesco Bank.[25] In May 2019, hackers stole more than 7,000 bitcoin from crypto exchange Binance, the world's largest by volume.[26]

II. Lack of Preparation

Despite these threats, mindsets are unprepared. Citizens see the internet as a free space; more security comes as a burden to them.[27] Many companies do not develop security by design; they create digital innovations and develop and use new digital technologies but rarely think about the security side of these technologies. It is, therefore, no surprise that sixty-one percent of cyber-attacks and sixty-five percent of data-breaches took weeks or more to discover.[28]

And States? According to the European Union Agency for Cybersecurity (ENISA),[29] governments tend to tolerate malicious activity as long as it stays at acceptable levels, meaning less than 2% of national income.[30] The discrepancy between the gains of internet—visible, real, for example, access to the world via smartphones—and the losses—virtual, more diffuse, and less tangible—at least so far leads to a form of apathy and indifference. There is growing acceptance that the internet comes with certain risks.[31]

Rapidity and inventiveness of attackers require new forms of acting for public authorities. Internet and cyber threats evolve very quickly. Spams and adware, widely used a few years ago, are mostly under control. But new threats are emerging every day, such as ransomware,[32]

[20]Kelly Bissell, Ryan M. Lasalle & Paolo Dal Cin, Ninth Annual Cost of Cybercrime Study 12 (2019), https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50. *See also* Webley & Hardy, *supra* note 9, at 353.

[21]For a review of past cyber-incidents involving financial institutions, see Tim Maurer, Ariel Levite, & George Perkovich, *Toward a global norm against manipulating the integrity of financial data* 23–40 (Kiel Institute for the World Economy, Economics Discussion Papers No 2017-38, 2017), http://www.economics-ejournal.org/economics/discussionpapers/2017-38.

[22]*Cybersecurity, Cyber Risk and Financial Sector Regulation and Supervision*, World Bank (Feb. 24, 2018), https://www.worldbank.org/en/topic/financialsector/brief/cybersecurity-cyber-risk-and-financial-sector-regulation-and-supervision.

[23]Jessica Silver-Greenberg, Matthew Goldstein & Nicole Perlroth, *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. Times (Oct. 2, 2014), https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/.

[24]Victor Mallet & Avantika Chilkoti, *How cyber criminals targeted almost $1bn in Bangladesh Bank heist*, Financial Times (Mar. 18, 2016), https://www.ft.com/content/39ec1e84-ec45-11e5-bb79-2303682345c8.

[25]Jill Treanor, *Tesco Bank cyber-thieves stole £2.5m from 9,000 people*, The Guardian (Nov. 08, 2016), https://www.theguardian.com/business/2016/nov/08/tesco-bank-cyber-thieves-25m.

[26]Eric Lam, *Hackers Steal $40 Million Worth of Bitcoin from Binance Exchange*, Bloomberg (May 8, 2019), https://www.bloomberg.com/news/articles/2019-05-08/crypto-exchange-giant-binance-reports-a-hack-of-7-000-bitcoin.

[27]European Political Strategy Centre (EPSC), *Building an Effective European Cyber Shield*, EPSC Strategic Notes, May 8, 2017, at 4.

[28]Kopp, Kaffenberger & Wilson, *supra* note 8, at 5; EPSC, *supra* note 27, at 4.

[29]Formerly: European Union Agency for Network and Information Systems.

[30]Dan Tofan, Theodoros Nikolakopoulos & Eleni Darra, The Cost of Incidents Affecting CIIs 5, 23 (2016), https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis/at_download/fullReport.

[31]EPSC, *supra* note 27, at 5.

[32]*See Id.* at 2 (noting ransomware is a type of malicious software designed to block access to a computer system to extort or blackmail the victim).

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

denial of service (DoS) attacks,[33] or phishing.[34] The mass of potential hackers today forms a hydra—closing down one platform or getting hold of one attacker can trigger two new platforms to open, or many more hackers applying the same technique, or others, within hours.

C. Key Elements for Effective Cybersecurity Regulation

In order to counter these threats, effective cybersecurity regulation is of growing importance. As a regulatory object, cybersecurity has specific characteristics and presents unique challenges. Their identification will help establish a set of key elements that cybersecurity regulation must respect in order to be effective.

I. General Observations and Elements

1. Manifold Forms of Cybersecurity

Cybersecurity comes in very different forms. Strengthening cyber resilience across different sectors, therefore, requires a variety of measures that must cover many different content elements. At the level of individual businesses, an effective cybersecurity framework addresses the prevention and detection of, the response to, and the recovery from a cyber-attack. It contains provisions on governance, such as risk assessment and management, regular system testing—for example, via simulated cyber-attacks—internal control mechanisms, and continuity planning, as well as provisions on independent review, incident reporting, and third party risks—altogether, essential elements of an effective cybersecurity framework.

2. Importance of the Human Element

Cybersecurity is not only about technology. Often, businesses and institutions are overly focused on technological security and software, but they neglect company culture, people, and processes. The human element, however, is still the weakest link when it comes to cybersecurity.[35] Vulnerabilities are introduced both in terms of what we regularly do, for example, opening e-mails or clicking on links, as well as what we fail to do, for example, updating systems or maintaining backups.[36] Effective cybersecurity regulation recognizes the importance of education and places emphasis on management and staff training, continuous learning, and risk-awareness-raising.[37]

3. Rapidly Changing Risk Landscape

Cyber risk is dynamic and evolves quickly. Technological advances enable cyber criminals to continuously develop and apply new methods to attack and compromise information and communication technology (ICT) systems.[38] Defense mechanisms must keep up with these developments. Effective cybersecurity regulation, therefore, obliges organizations to continuously update their cybersecurity arrangements. At the same time, it does not impose too many or too detailed requirements but leaves space for flexible and individual solutions, thereby promoting agility

[33]*See* Kopp, Kaffenberger & Wilson, *supra* note 8, at 5 (highlighting that DoS attacks do not involve direct stealing of data or money, but compromise the attacked firm's provision of services to customers as websites are knocked offline as the website is overwhelmed with traffic).

[34]Phishing is the fraudulent practice of sending emails to induce individuals to reveal personal information, such as passwords or credit card numbers. *See* EPSC, *supra* note 27, at 5.

[35]Webley & Hardy, *supra* note 9, at 353; Bissell, Lasalle & Dal Cin, *supra* note 20, at 9; Press Release, *supra* note 19.

[36]Lorenzo Pupillo, Melissa K. Griffith, Steven Blockmans & Andrea Renda, *Strengthening the EU's Cyber Defence Capabilities*, Centre Eur. Pol'y Studies, 2018, at 8–9.

[37]*See also* Connolly, *supra* note 9, at 9.

[38]Financial Stability Board (FSB), Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices 1 (2017) https://www.fsb.org/wp-content/uploads/P131017-2.pdf.

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

and adaptability.[39] In the absence of a one-size-fits-all solution to the challenges ahead, organizations must be able to put in place and maintain technologies, mechanisms, and procedures that are specifically tailored to their individual needs, systems, employees, and risk profiles.[40] Flexibility also enables institutions to balance proportionality and costs as key drivers of any cybersecurity arrangements to be adopted. Considering the rapidly changing nature of cyber risks, overly specific technical requirements also risk being obsolete faster than they can be repealed and replaced by the regulator. Eventually, a certain degree of regulatory flexibility would facilitate the development of innovative cybersecurity solutions, enabling organizations to always stay one step ahead of cyber-criminals.

4. Importance of Cooperation and Information Sharing

In order to best anticipate and respond in a consistent manner to cyber-attacks, a multidisciplinary approach and information sharing are required.[41] There is a need to shift from building static capabilities to more proactive detection of threats. The challenge will be to detect cyber threats in advance and to isolate them in the system to best understand their functioning and potential impact before reacting. This requires the full collaboration of the different sectors of society, including the private sector, particularly with regard to critical infrastructures.[42] Cooperation and information sharing within the private sector, between the private and the public sector, and at the public level are of particular importance. At best, such mechanisms are established on a cross-sectoral and cross-border basis to avoid a "siloed approach." Types of information to be shared include, but are not limited to, cyber-incidents, new cyber threats, vulnerabilities in software, hardware or processes, mitigation methods, best practices, and strategic analysis.[43]

II. Observations and Elements with Particular Regard to the Financial Sector

1. Interconnections and Interdependencies in the Financial Sector

More than many other industries, the financial sector and its systems are highly interconnected and interdependent.[44] As a result, a cyber-attack can spread very quickly among financial system participants. What is more, the financial sector is only as cybersecure as its weakest link. The failure of one participant, a "single point of failure," can easily affect and impede the services provided by other participants. Due to the interconnectedness of the sector, a small-volume participant or a business providing non-critical financial services may be as risky as a major participant or a critical financial services provider.[45] Effective cybersecurity regulation, therefore, covers all actors of a particular sector, and it is not limited to the largest or most relevant financial institutions or sub-sectors.[46] It also covers more general services that are relevant to the financial sector, such as electricity provision.

[39]Flexibility describes the number of implementation paths companies have available for compliance. *See* Jacques Pelkmans & Andrea Renda, *Does EU Regulation Hinder or Stimulate Innovation?*, CENTRE EUR. POL'Y STUD., 2014, at 5, 12. For different legislative tools to build in more flexibility into regulation, see *infra* text accompanying notes 192–195. *See also* Amitai Etzioni, *The Private Sector: A Reluctant Partner in Cybersecurity*, 15 GEO. J. INT'L AFF. 69, 71–72 (2014).

[40]Sales, *supra* note 2, at 1545–46; FSB, *supra* note 38, at 18. This also reflects the principle of proportionality.

[41]*See also* Sales, *supra* note 2, at 1546.

[42]EPSC, *supra* note 27, at 13.

[43]*See* ENISA, INFORMATION SHARING AND ANALYSIS CENTRES (ISACS): COOPERATIVE MODELS 31–32 (2018), https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models/at_download/fullReport.

[44]*See*, *e.g.*, Antoine Bouveret, *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment* 11 (International Monetary Fund, Working Paper No. 18/143, 2018).

[45]EUR. CENT. BANK, CYBER RESILIENCE OVERSIGHT EXPECTATIONS FOR FINANCIAL MARKET INFRASTRUCTURES 2 (2018), https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf.

[46]*See also* AQUILES A. ALMANSI, FINANCIAL SECTOR'S CYBERSECURITY: REGULATIONS AND SUPERVISION 25 (World Bank Group, 2018), http://documents1.worldbank.org/curated/en/686891519282121021/pdf/123655-REVISED-PUBLIC-Financial-Sectors-Cybersecurity-Final-LowRes.pdf ("Due to the contagion potential derived from the interconnected nature

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

2. Broad Range of Entry Points and Third Party Participants

The financial system is a complex network of participants from different environments and shared technologies. It is not only comprised of financial institutions, but also third-party service providers—for example, cloud-service providers—with whom financial institutions work. With regard to these cloud-service providers, only a limited number of big players dominate the market. This leads to concentration risks.[47] Moreover, financial institutions increasingly rely on information systems in the provision of financial services and their day-to-day operations.[48] Services are increasingly instant and globally available. Due to progress made in cloud computing, the Internet of Things, and 5G-technologies, the number of devices, networks, and interfaces used in the daily business of a financial institution has increased significantly. This results in a broad range of entry points for possible cyber-attacks, both at the technological level and at the level of participants.

Against this background, effective cybersecurity regulation needs to cover new technologies as well as third-party cyber risks. In the context of the latter, it must set out the conditions according to which financial institutions may enter into outsourcing agreements with third-party service providers and the requirements concerning the management and monitoring of the according risks. It must also provide for the possibility of supervisory access to a financial institution's third-party service providers. This onsite access can be obtained either directly in the applicable law or by requiring the financial institution to include this right in outsourcing contracts. Direct supervision of third-parties must also be considered.

3. Importance of the Precautionary Principle

Due to the rapidly changing nature of cyber risks and the uncertainties about future technical developments and threat scenarios, cybersecurity regulation must put particular emphasis on risk prevention. In this context, the precautionary principle is of particular importance. The European Commission and the European Court of Justice consider the precautionary principle to be a general legal principle of EU law.[49] In the context of financial stability and cybersecurity, the precautionary principle requires government action already when there is a *risk* to the stability of the financial system. The mere possibility of damage is enough; a concrete probability is not required. In this situation, and considering the principle of proportionality, governments must adopt procedural instruments, such as notification requirements about cyber-incidents, in order to generate information. Should these instruments be insufficient to mitigate the risk, measures that are more intrusive must be considered.[50]

---

of contemporary financial infrastructure, traditional concepts such as "proportionality" in regulatory requirements and supervisory attention … may have to be revised. An interconnected system is as strong as its weakest link. Hence, it may be necessary to set minimum cybersecurity standards for all institutions, independently of other dimensions of their systemic importance.").

[47]Eur. Supervisory Auth., Joint Advice of the European Supervisory Authorities: To the Commission on the Need for Legislative Improvements Relating to ICT Risk Management Requirements in the EU Financial Sector, at 17–18, JC 2019 26 (Apr. 10, 2019).

[48]*Id.* at 7.

[49]*European Commission, Communication on the Precautionary Principle*, COM (2000) 1 final (Feb. 2, 2000); ECJ, Case C-77/09, Gowan Comércio Internacional e Serviços Lda v. Ministero della Salute, ECLI:EU:C:2010:803 (Dec. 22, 2010), para. 72, http://curia.europa.eu/juris/liste.jsf?language=en&num=C-77/09; ECJ, Case C-180/96, United Kingdom v. Comm'n ECLI:EU:C:1998:192 (May 5, 1998), paras. 98–100, http://curia.europa.eu/juris/document/document.jsf?docid=43817&doclang=EN; ECJ, Case C-157/96, Nat'l Farmers' Union, ECLI:EU:C:1998:191 (May 5, 1998), paras. 62–64, http://curia.europa.eu/juris/liste.jsf?language=en,T,F&num=157/96.

[50]Christian Calliess, *Finanzkrisen als Herausforderung der internationalen, europäischen und nationalen Rechtsetzung*, 71 VVDStRL 113, 139–41 (2012).

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

III. Division of Labor Between the Private and the Public Sector

In complex regulatory fields like cybersecurity in the financial sector, knowledge based on expertise and information is a precondition for every kind of state activity. This applies *a fortiori* in the present context—public authorities often are not as advanced as the private sector when it comes to cybersecurity.[51]

The shortcomings of command and control legislation in complex policy fields such as cybersecurity, as well as the central role of information and knowledge, make the cooperation of public authorities with private actors a necessity ("private-public engagement").[52] In the context of the concretization of public goods, such as the stability of the financial system and cyber resilience,[53] this is to be understood as the result of a process of the division of labor in which both governmental and private actors contribute in all phases of implementation.[54] These comprise, for example, contributions to fact investigations, or expertise; the creation of standards by private self-regulatory entities; private self-control of safety standards; and the creation of private organizational structures to achieve government goals, such as private contributions to infrastructure maintenance and safety. Indeed, the private sector, both in the form of critical infrastructure operators and standard setters, currently stands in the frontline of fighting cyber-attacks against the financial sector.

From a public law perspective—based on the state responsibility to deliver on public goods—a central task becomes the regulation of the private contributions in collaborative structures to ensure an overall outcome that promotes the public interest.[55] In this regard, German administrative law theory defines a differentiated concept of public responsibility based on three levels of public responsibility.

1. Comprehensive State Responsibility

The first level is defined by a comprehensive state responsibility (*Erfüllungsverantwortung*) that ensures the public good by public administration and state authorities acting based on the classical command and control legislation.

2. Collaborative Approach

The second level is defined by a collaborative approach between the public sector and private actors based on a public responsibility with regard to objectives and results. For this kind of cooperation between the public and the private sector, German administrative law theory coined the terms of "*Gewährleistungsverantwortung*" and "*Gewährleistungsverwaltungsrecht*" defining an essential element of regulatory law.[56] Their function is to safeguard the public good by framing the "procedure" of decision-making that is primarily based on private expertise, collaborative action, and organization. In this context, the dynamic adaptation of legal demands on technical developments and the need for opportunities to review and/or revise decisions made under

[51]See Nathan A. Sales, *Privatizing Cybersecurity*, 65 UCLA L. Rev. 620, 628, 631–33 (2018).

[52]*See generally* David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 Ga. St. U. L. Rev. 287 (2014). For the U.S. perspective, see Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 Tex. L. Rev. 467 (2017); Paul Rosenzweig, Cybersecurity and Public Goods: The Public/Private "Partnership" (Hoover Inst., 2012), https://www.hoover.org/sites/default/files/research/docs/emergingthreats_rosenzweig.pdf.

[53]George Christou, *The Collective Securitisation of Cyberspace in the European Union*, 42 West Eur. Pol. 278, 280 (2019) speaks of cybersecurity as a "collective public good." *See also* Benoît Cœuré, *Cyber Resilience as a Global Public Good*, Eur. Central Bank (May 10, 2019), https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190510_2~2e988cb439.en.html (Speech at the G7 conference).

[54]Such a division of labor is also advocated by Sales, *supra* note 2, at 1517–19, 1547.

[55]In the context of cybersecurity, see Hannfried Leisterer, Internetsicherheit in Europa 34–37 (2018).

[56]Calliess, *supra* note 50, at 124; Leisterer, *supra* note 55, at 34–37. *See generally* Andreas Voßkuhle, *Beteiligung Privater an der Wahrnehmung öffentlicher Aufgaben und staatliche Verantwortung*, 62 VVDStRL 266 (2003).

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

conditions of uncertainty are key elements of the legal framing that has to ensure that the state finally delivers on the public good.

3. Umbrella Responsibility

The third level of public responsibility is a kind of umbrella, and it entitles state authorities to intervene as soon as the collaborative approach leads to shortcomings in delivering on the public good (*Auffangverantwortung*).

The three levels of public responsibility do not define a hierarchical order but rather different ways and tools through which the legislator can deliver on a public good, such as the stability of the financial system, by avoiding the shortcomings and disadvantages of command and control legislation in complex policy fields. With regard to the protection against cyber threats, the responsibility for the stability of the financial system is assumed in close cooperation between the Member States and the EU (*Daseinsvorsorgeverbund*), and in collaboration with the private sector.[57]

D. General Observations on the Legal Framework for Cybersecurity in the Financial Sector

In light of the foregoing, the question thus arises whether—and to what extent—the current regulatory landscape for cybersecurity in the financial sector already addresses the challenges identified and reflects the requirements established.

Today, the overall legal framework for cybersecurity in the financial sector is characterized by a multilevel structure, a variety of legal sources, and a wide range of different rule makers and involved actors.[58]

I. Multilevel and Multistakeholder Structure

Provisions on cybersecurity in the financial sector exist at the international, European, and national level. They are developed by national and international standard-setting bodies, international organizations, and national as well as supranational legislators and supervisors. In recent years, development activity has increased significantly. The organizational picture is completed by transnational fora and regional, non-governmental, and independent private organizations.[59] Responsibilities between these actors are not always clearly delineated.[60]

The scope of the various schemes on cybersecurity differs considerably. While some pursue a cross-sectoral approach, others specifically address cybersecurity in the financial sector or even target certain subsectors such as banks or payment systems. A survey of the Financial Stability Board (FSB) conducted in 2017 showed that all member jurisdictions of the FSB, including the EU, address banks and financial market infrastructures, and a majority of jurisdictions address trading venues, insurance companies, broker-dealers, and asset managers.[61]

[57]*See generally* Philipp Steinberg, *Daseinsvorsorge im europäischen Mehrebenensystem als geteilte Gewährleistungsverantwortung*, *in* Recht und Ökonomik 189 (Marc Bungenberg et al. eds., 2004).

[58]For a periodically updated compilation of publicly released regulations and guidance on cybersecurity in the financial sector, see World Bank, Digest of existing and proposed regulations on cybersecurity preparedness (3d ed. 2019); *see also* Basel Committee on Banking Supervision (BCBS), Cyber-Resilience: Range of Practices (2018); FSB, *supra* note 38.

[59]For an overview of private organizations that are active in the field of cybersecurity, see Bendiek & Porter, *supra* note 13, at 171–72.

[60]*Id.* at 167.

[61]FSB, *supra* note 38, at 1–2, 5.

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

II. Different Regulatory Strategies

In general, cybersecurity in the financial sector is addressed either by targeted provisions on cybersecurity and/or IT risk, or by provisions that address operational risk in financial institutions generally. Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people, and systems or external events.[62] Among FSB member jurisdictions, sixty-six percent of reported schemes took a targeted approach to cybersecurity, IT risk, or both, while thirty-four percent addressed operational risk generally. For FMIs and banks, the percentages of reported targeted regulatory schemes were seventy-seven and seventy-one percent, respectively.[63] In addition, FSB member jurisdictions mainly described their regulatory schemes on cybersecurity as principles-based,[64] as opposed to rule-based.[65]

III. Various Content Elements

Content-wise, the different schemes and provisions often overlap. Elements that FSB member jurisdictions address most frequently are: Risk assessment; regulatory reporting; role of the board; third-party interconnections; system access controls; incident recovery; testing; training; creation of role responsible for cybersecurity, such as chief information security officer; information sharing; expertise of the board or senior management; and cyber risk insurance.[66]

IV. Different Types of Provisions, Especially: Standards

1. General Overview

Provisions on cybersecurity in the financial sector take very different forms and differ considerably in legal nature and effect. While some instruments impose mandatory requirements, others provide voluntary guidance or combine both.

At the national level, provisions of both legally binding and non-binding nature exist. According to the 2017 FSB survey, all FSB member jurisdictions have publicly released regulations or guidance that address cybersecurity for at least parts of the financial sector.[67] In jurisdictions where no specific cybersecurity regulation for the financial sector is in place, supervisors encourage financial institutions to implement international standards and guidance.[68]

At the international level, private self-regulatory entities, networks of specialized administrative bodies, and international organizations have developed cybersecurity standards of various forms and legal quality to help improve cybersecurity in the financial sector. Contributing to the risk management of financial institutions, they establish common security requirements and capabilities needed for secure solutions.[69] These standards play a predominant role with regard to the different types of provisions constituting the legal framework for cybersecurity in the financial sector.

2. Standards

The phenomenon of private self-regulatory entities, informal networks of specialized administrative bodies, and international organizations creating standards is widespread in areas where highly

[62]Basel Committee on Banking Supervision (BCBS), Principles for the Sound Management of Operational Risk 3 (2011).

[63]FSB, *supra* note 38, at 2.

[64]*Id.*

[65]For more details on the rule-based and the principle-based approach, see *infra* text accompanying notes 192–194.

[66]Listed in descending order, FSB, *supra* note 38, at 2–3.

[67]*Id.* at 1.

[68]BCBS, supra note 58, at 9.

[69]Shin-yi Peng, *"Private" Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime*, 51 Cornell Int'l L.J. 445, 446 (2018).

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

technical and rapidly evolving matters are involved—such as the regulation of financial markets[70]—especially with regard to cybersecurity. Far from being a new phenomenon, stemming from the beginnings of globalization and, therefore, much older than European integration, it is one of the most popular examples for new international and European governance structures.

2.1 Definition and Types of Standards

Standards set out what are widely accepted as good principles, practices, or guidelines in a given area.[71] The standardization of products, services, or processes is traditionally conducted by technical bodies that primarily represent the vested interests with their expertise.

From an implementation perspective, standards differ in their specificity. As fundamental tenets concerning a broad policy area, *principles* are usually set out in a general way offering a degree of flexibility in implementation to suit country circumstances.[72] *Practices* are more specific and concretize the practical application of the principles within a more narrowly defined context.[73] Finally, *guidelines* provide detailed guidance on steps to be taken or requirements to be met in a particular area.[74] They are specific enough to allow a relatively objective assessment of the degree of observance.[75]

From a practical perspective, international standards can be seen as a "substitute" for hard international law,[76] making lengthy and costly negotiations between states obsolete.[77] The expertise involved in the drafting process ensures the development of high-quality standards, which usually leads to high acceptance rates within the community to which they are addressed.

2.2 Legal Effects of Standards and Implementation Paths

As soft law instruments,[78] standards are not formally binding and do not impose direct obligations on regulators, supervisors, or private entities. On a voluntary basis, however, international standards are often implemented by the industry they are addressed to, thereby developing *de facto* binding effects.[79] International standards also frequently serve as a model for legislative and regulatory activity at the national or EU level, either being substantially copied into by incorporation, or dynamically referred to in binding provisions by reference. This way, they contribute to reducing risks of regulatory arbitrage and, depending on the degree of implementation, to achieving at least some degree of international convergence of cybersecurity regulation and supervision in the financial sector.

According to the 2017 FSB survey, all member jurisdictions of the FSB, including the EU, drew upon previously developed international standards when they developed their own cybersecurity regulatory and supervisory schemes for the financial sector.[80]

[70]Anne van Aaken, *Democracy in Times of Transnational Administrative Law: The Case of Financial Markets*, *in* PERSPECTIVES AND LIMITS OF DEMOCRACY 41, 41 (Harald Eberhard, Konrad Lachmayer, Gregor Ribarov & Gerhard Thallinger eds., 2008).

[71]*Id.* at 46; Financial Stability Board (FSB), *The Compendium of Standards*, https://www.fsb.org/work-of-the-fsb/about-the-compendium-of-standards/ (last visited Jan. 21, 2020).

[72]van Aaken, *supra* note 70, at 46

[73]*Id.*

[74]*Id.*

[75]*Id.* at 47. Terminology in this context varies considerably.

[76]*Id.* at 51.

[77]Calliess, *supra* note 50, at 132.

[78]For a definition and an overview of different types of soft law, see Dinah Shelton, *Soft Law*, *in* HANDBOOK OF INTERNATIONAL LAW 68, 69 (David Armstrong ed., 2008). For the advantages and disadvantages of soft law, refer to Chris Brummer, *Why Soft Law Dominates International Finance—And Not Trade*, 13 J. INT'L ECON. L. 623 (2010).

[79]Calliess, *supra* note 50, at 125.

[80]FSB, *supra* note 38, at 2.

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

2.3 Challenges of Private Standard Setting, Especially: Democratic Legitimacy

Against this background—*de facto* binding effects of standards and standards as a model for subsequent legislative activity—it is of importance that standard-setting processes comply with the minimum requirements of democratic legitimacy.

a) The Notion of Democratic Legitimacy

In academia, different notions of democratic legitimacy are being discussed. Depending on the position taken, the assessment and evaluation of the standard-setting process will differ. Within the scope of this Article, it is impossible to do justice to the rich literature on this topic.[81] Here, an input-orientated notion will be combined with an output-oriented notion of democratic legitimacy.[82] The input-oriented notion can be summarized as government *by* the people. Democratic legitimacy is derived from the community of people, whether they are specifically affected by the provisions in question or not.[83] Output-oriented notions of democratic legitimacy stress the aspect of government *for* the people where the outcome of the political process, hence the quality of laws, is of main importance. Under this concept, the participation of experts in order to guarantee "good laws" is wholly accepted, if not required.[84]

b) Minimum Legitimacy Requirements for Standard Setting

Against this background, standards and standard-setting processes that involve experts are, in principle, desirable. Although, they have to fulfill certain minimum requirements. At first, transparency *vis-à-vis* the public, the European and national parliaments must be ensured. Such transparency must go hand in hand with a formalization of the drafting process through procedural rules, an obligation to state reasons, documentation obligations, and fit and proper requirements for all experts involved.[85] Comments received must be adequately considered in the drafting process.[86] Finally, equal participation rights in the consultation process for *all* interested parties, not only those affected, must be safeguarded, taking account of the different organizability of different interests.[87]

c) Consequences

As long as standard-setting processes do not meet these minimum requirements, even *de facto* binding effects of standards are problematic. To resolve this problem, standard-setting bodies must make arrangements and adopt procedures in order to comply with the minimum requirements outlined above; or the respective standards must be substituted by statutory provisions adopted in a legislative procedure.

Legislators, however, cannot simply refer to or directly incorporate standards that have not been developed under a procedure that complies with the minimum requirements of democratic legitimacy. Instead, they must carry out an in-depth analysis and own substantive assessment of the respective standards before referencing them or incorporating them in binding legislation.[88]

One may respect the standardization structure as a helpful institutional solution to a regulatory problem, and one should not try to reduce the structure to its public or private aspects. Neither a purely governmental nor a purely civil arrangement seems to work better. But this does not imply

[81]For an overview, see van Aaken, *supra* note 70, at 51.

[82]For a similar approach, see Gregor Bachmann, *Globale Finanzmarktregulierung als Herausforderung des Rechts*, *in* Finanzmarktregulierung Zwischen Innovation und Kontinuität in Deutschland, Europa und Russland 1, 3, 21 (Gregor Bachmann & Burkhard Breig eds., 2014).

[83]van Aaken, *supra* note 70, at 52.

[84]*Id.* at 53.

[85]Calliess, *supra* note 50, at 133.

[86]*Id.*

[87]van Aaken, *supra* note 70, at 55.

[88]Calliess, *supra* note 50, at 133–34. Critical of such a requirement is Bachmann, *supra* note 82, at 15.

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

that it is impossible to develop mechanisms that address legitimacy problems of standardization more adequately, especially procedures concerning the inclusion of interests and the transparency of the rulemaking process. This benevolent approach accepts standardization bodies as a genuine form of governance that can complement but not substitute government structures.

2.4 Overview of International Cybersecurity Standards

International cybersecurity standards for the financial sector have been developed by many different actors.

a) G7 CEG Fundamental Elements of Cybersecurity for the Financial Sector

In 2016, the G7 Cyber Expert Group (G7 CEG) published its Fundamental Elements of Cybersecurity for the Financial Sector,[89] a set of high-level principles designed to help address cyber risks facing the financial sector. The G7 has no binding decision making competences and is not an international organization; at most, it is a "soft organization."[90] As high-level building blocks, its principles and other publications are frequently concretized into standards that are more detailed and then referred to or incorporated in binding legislation at the EU or national level, known as a "cascade mechanism."

Based on the 2016 Elements, the 2017 G7 CEG Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector[91] provide additional guidance on good cybersecurity practices for institutions. In 2018, the G7 CEG published its Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector[92] and its Fundamental Elements for Threat-Led Penetration Testing.[93]

b) CPMI-IOSCO Principles for Financial Market Infrastructures

Specifically addressed to FMIs, the Committee on Payments and Market Infrastructures of the Bank for International Settlements (CPMI)[94] in 2012 issued, jointly with the International Organization of Securities Commissions (IOSCO), its Principles for Financial Market Infrastructures (PFMI)[95] in order to harmonize and strengthen the existing international standards for FMIs. CPMI is the global standard-setter for payments, clearing, and settlement; its members are central banks. It does not possess any formal supranational authority.[96] IOSCO is an international body that brings together the world's securities regulators. The PFMI are expressed as broad and flexible principles. In 2016, the PFMI were complemented by the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures.[97]

c) ISO/IEC 27000 Family of Standards on Information Security Management Systems

An important cross-sectoral set of standards for cybersecurity is the ISO/IEC 27000 Family of Standards on Information Security Management Systems[98] published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The ISO is a non-governmental international organization composed of representatives from 163 national standard bodies. The ISO/IEC 27000 Family of Standards is meant to help

[89]G7 Conference, Fundamental Elements of Cybersecurity for the Financial Sector (2016).

[90]With regard to the G20, see Calliess, *supra* note 50, at 126.

[91]G7 Conference, Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector (2017).

[92]G7 Conference, Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector (2018).

[93]G7 Conference, Fundamental Elements for Threat-Led Penetration Testing (2018).

[94]Officially named Committee on Payment and Settlement Systems (CPSS) prior to Sept. 2014.

[95]CPMI-IOSCO, Principles for Financial Market Infrastructures (2012).

[96]CPMI Charter art. 3.

[97]CPMI-IOSCO, Guidance on Cyber Resilience for Financial Market Infrastructures (2016).

[98]ISO/IEC, ISO/IEC 27000:2018 (2018).

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

organizations develop and implement a framework for managing the security of their information assets and information entrusted to them by customers or third parties.[99]

d) NIST Framework for Improving Critical Infrastructure Cybersecurity

With its Framework for Improving Critical Infrastructure Cybersecurity,[100] the US National Institute of Standards and Technology (NIST), an agency of the United States Department of Commerce, developed a set of cross-sectoral principles, practices, and guidelines to manage cybersecurity-related risks. By referencing globally recognized standards, the framework can be used not only within the US but also by organizations across the world.

e) Further International Standard Setters

There are several other international standard-setting bodies, associations, and networks that have issued soft law instruments on cybersecurity in the financial sector. The most important of these are: The Basel Committee on Banking Supervision (BCBS),[101] an informal network of public authorities in the area of technical expertise; the Organization for Economic Co-Operation and Development (OECD),[102] an international organization; and the Global Financial Markets Association (GFMA),[103] a forum for the largest globally active financial and capital market participants. Finally, the Information Systems Audit and Control Association (ISACA), an international association, engages in the development, adoption, and use of globally accepted, industry-leading knowledge and practices for information systems.

E. Cybersecurity in the Financial Sector at EU Level

Having established the broader overall picture of the legal framework for cybersecurity in the financial sector, this Section will analyze the legal cybersecurity landscape within the EU. After a quick look at the scope and limits of EU competences in this area, it will focus on the regulatory framework and the corresponding governance structures for cybersecurity at the EU level.

I. EU Competence Framework

1. EU Cybersecurity Regulation and the Principle of Conferral, Article 5(2) TEU

Under the principle of conferral, the Union shall only act within the limits of the competences conferred upon it by the Member States in the Treaties, and in order to attain the objectives set out therein.

European cybersecurity legislation has already been based on several legal bases in the Treaties.[104] These include the internal market (Article 114 TFEU); the right of establishment

[99]FSB, *supra* note 38, at 49.

[100]NIST, Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1., 2018). *See generally* Scott J. Shackelford, Andrew A. Proia, Brenton Martell & Amanda N. Craig, *Toward a Global Cybersecurity Standard of Care: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 Tex. Int'l L.J. 305 (2015); Lei Shen, *NIST Cybersecurity Framework: Overview and Potential Impacts*, 10 SciTech L. 16 (2014).

[101]Already in 2003, the BCBS adopted the final version of its Risk Management Principles for Electronic Banking. In 2011, the BCBS published its Principles for the Sound Management of Operational Risk.

[102]*See Recommendation of the Council on Digital Security of Critical Activities*, OECD/LEGAL/0456 (Dec. 11, 2019); *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*, OECD/LEGAL/0415 (Sept. 17, 2015).

[103]*See, e.g.*, Global Financial Markets Association (GFMA), Framework for the Regulatory Use of Penetration Testing in the Financial Services Industry (2018).

[104]Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, 2016 O.J. (C202), 13, 2016 O.J. (C202) 1 [hereinafter TEU and TFEU]. For secondary law examples, see *infra*, footnotes beginning at note 112.

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

and the freedom of services (Articles 62, 53(1) TFEU); the smooth operation of payment systems (fourth ident of Articles 127(2), 132(1) TFEU); and the area of freedom, security, and justice (Article 83(1) TFEU). With regard to coordination at the EU level, a more general legal basis is provided for in Article 74 TFEU.[105]

Cyber policy, especially in the context of the protection of critical infrastructures and the guarantee of financial stability, has a security dimension. The Member States, however, are traditionally reluctant to share competences in this regard.[106] Indeed, Article 4(2) TEU points out that the EU shall respect the "essential State functions, including … maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State." Does this preclude any EU action in the field of cybersecurity?

There are strong arguments that this is not the case. Article 4(2) TEU refers only to "national security," meaning that it does not preclude measures referring to "Schengen security," defined by cross-border effects of internal security.[107] With cyberspace and cyber aggressions being borderless, there is good reason to assume that cybersecurity is not to be regarded as a purely internal security matter but must rather be assigned to "Schengen security." This applies *a fortiori* in the context of guaranteeing financial stability, which itself has a cross-border dimension. Moreover, cybersecurity can be attributed to the area of freedom, security, and justice (Article 67 TFEU), which Art 4(2)(j) TFEU lists as a "shared competence between the Union and the Member States."[108]

What is more, the creation of a Digital Single Market for (financial) services (Art. 114 TFEU), including the establishment of a robust and resilient Banking and Capital Markets Union, is a core task of the EU, which can only be realized in a cybersecure digital environment. Cybersecurity is a *conditio sine qua non* for the future development of the Digital Single Market. EU competences in these areas, therefore, go hand in hand with EU competences in the field of cybersecurity in its European dimension.

2. EU Cybersecurity Regulation and the Principle of Subsidiarity, Article 5(3) TEU

In areas that do not fall within the exclusive competence of the Union, the principle of subsidiarity must be observed. This also applies to the area of cybersecurity. Union action in this field must, therefore, pass the subsidiary test. In order to pass this test, it is first necessary that the objectives of the proposed action cannot be sufficiently achieved by the Member States ("necessity" criterion), and second, that the action can more successfully be undertaken at the Union level ("added value" criterion). Although compliance must be assessed on a case-by-case basis, some general observations can be made.

Due to the transnational nature of cyber threats and the cross-border interdependencies between network and information systems, unilateral approaches to cybersecurity at Member State level are often inefficient. Diverging national regulatory requirements on cybersecurity in the financial sector also prevent the establishment of a level playing field among financial institutions in the EU and risk leaving legislative loopholes. Finally, in the absence of harmonization, financial institutions with cross-border operations risk having to comply with different regulatory standards in different Member States concerning the same aspect of cybersecurity (together: "necessity" criterion). An EU-wide approach establishing minimum requirements on cybersecurity could, at least to some extent, answer these problems ("added value" criterion). There is thus still sufficient leeway for future European legislation from a principle of subsidiarity point of view.

[105]Christou, *supra* note 53, at 279 (EU cybersecurity governance emerged "across three distinct but interrelated mandates: Freedom, Justice and Security …, the Internal Market, and the Common Security and Defence Policy …").

[106]Carrapico & Barrinha, *supra* note 11, at 1264; Pupillo, Griffith, Blockmans & Renda, *supra* note 36, at 3; EPSC, *supra* note 27, at 9.

[107]EPSC, *supra* note 27, at 9.

[108]*Id.*

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

II. EU Regulatory Framework

Although the impact of cyber threats is still neglected to a remarkable extent, the EU is not entirely unprepared. At the EU level, provisions on cybersecurity in the financial sector are set out in legislative acts, notably regulations and directives; administrative rules, such as delegated acts and regulatory technical standards; and recommendations and guidelines. Due to limited space, it is impossible to establish a comprehensive picture of cybersecurity regulation in the financial sector. The following subsection, therefore, analyzes EU cybersecurity regulation with regard to systemically important payment systems and credit institutions as reference areas.

1. Regulation of Systemically Important Payment Systems (SIPS)

Payment systems facilitate the clearing, settlement, and recording of payments, thereby contributing to maintaining and promoting financial stability and economic growth.[109] As financial markets infrastructures, however, they also concentrate risk.[110] If not properly managed, they can become a source of financial shocks or a major channel through which these shocks are transmitted across domestic and international financial markets.[111]

The oversight of payment systems is an essential function of central banks. In the euro area, it is carried out by Eurosystem (Article 127(2) TFEU and Article 3.1 of the Statute of the ESCB and of the ECB). The Eurosystem has set out its oversight objectives in specific oversight schemes.

1.1 Overview of the Different Regulatory Schemes

For a large part, Eurosystem oversight of FMIs is based on the 2012 CPMI-IOSCO Principles for financial market infrastructures (PFMIs) and, regarding cybersecurity, in particular, the 2016 CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures.

a) SIPS Regulation

In 2014 and 2017, respectively, the ECB translated parts of this international standard into the "SIPS Regulation,"[112] which applies to payment systems of systemic importance in the euro area operated by both central banks and private operators. Under the SIPS Regulation, the ECB is currently responsible for overseeing TARGET2, EURO1, and STEP2-T. The Banque de France oversees CORE(FR). The SIPS Regulation has been based on Article 127(2) TFEU and Articles 3.1, 22, and 34.1 first indent of the Statute of the ESCB and of the ECB.

As one of only a few provisions in EU law, Article 15(4a) SIPS Regulation, entitled operational risk, explicitly lays down cybersecurity requirements. The paragraph, which has been added to the SIPS Regulation during its amendment in 2017, reads as follows.

A SIPS operator shall establish an effective cyber resilience framework with appropriate governance measures in place to manage cyber risk. The SIPS operator shall identify its critical operations and supporting assets, and have appropriate measures in place to protect them from, detect, respond to, and recover from cyber-attacks. These measures shall be regularly tested. The SIPS operator shall ensure it has a sound level of situational awareness of cyber threats. The SIPS operator shall ensure that there is a process of continuous learning and evolving to enable it to adapt its cyber resilience framework to the dynamic nature of cyber risks, in a timely manner, whenever needed.

[109] CPMI-IOSCO, *supra* note 95, at 5.

[110] *Id.*

[111] *Id.* at 5, 8.

[112] Regulation of the European Central Bank (EU) No. 795/2014 of 3 July 2014 on Oversight Requirements for Systemically Important Payment Systems, 2014 O.J. (L 217) 16, amended by Regulation (EU) No. 2017/2094 of the European Central Bank of 3 November 2017 Amending Regulation (EU) No. 795/2014 on Oversight Requirements for Systemically Important Payment Systems, 2017 O.J. (L 299) 11.

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

b) Cyber Resilience Oversight Expectations for Financial Markets Infrastructures (CROE)

Article 15(4a) SIPS Regulation is complemented by the ECB's Cyber Resilience Oversight Expectations for Financial Markets Infrastructures (CROE),[113] which set out detailed best practices to operationalize the rather abstract CPMI-IOSCO guidance. The CROE apply to all categories of payment systems, not only systemically important payment systems.[114] Recently, the CROE have been embraced by the World Bank with a view to promoting global harmonization and might, therefore, eventually be used around the world.[115]

c) General Data Protection Regulation (GDPR)

With a primary focus on ensuring the security of personal data—instead of network and information systems—EU data protection laws such as Articles 32–34 of the GDPR[116] require financial entities, including SIPS operators and credit institutions, to implement appropriate technical and organizational measures to prevent a cyber-incident and lay down notification requirements.[117]

1.2 Critical Assessment

Article 15(4a) SIPS Regulation establishes a clear, legally binding framework for cybersecurity for systemically important payment systems. The provision explicitly addressees governance and the most important cyber risk prevention and mitigation measures, stipulates regular testing, and requires SIPS operators to constantly learn and evolve; in other words, it does not neglect the human element either. Potential cyber risks resulting from the collaboration with third parties are covered in more general terms by Article 15(7) SIPS Regulation requiring a SIPS operator to "identify, monitor, and manage the risks that critical participants, other FMIs, and service and utility providers might pose to the SIPS' operations." Except for requirements on incident notification, the SIPS Regulation thus addresses all essential elements of an effective cybersecurity regulatory framework. In addition, the use of general terms such as "appropriate measures" and the emphasis put on the ability of operators to "adapt [their] cyber resilience framework to the dynamic nature of cyber risks" leaves sufficient room for operators to react with the necessary flexibility to dynamically evolving cyber threats. At the same time, these general terms allow for the development of new, innovative approaches to cybersecurity.

2. Regulation of Credit Institutions

The current regulatory landscape for credit institutions is more complicated. While the NIS Directive, the cyber-incident reporting framework of the ECB, and certain provisions of PSD2 and MiFID II make explicit reference to cybersecurity, other instruments only address cybersecurity on the edge or concern the management of the overall operational risk of a credit institution.

2.1 Overview of the Different Regulatory Schemes

a) NIS Directive

In 2018, Member States, together with the EU, set up a new regime for European cyber-protection. EU Directive 2016/1148, concerning measures for a high level of common security of network and information systems across the Union, is known as the "NIS Directive."[118] To date, the NIS

[113]Eur. Cent. Bank, *supra* note 45.

[114]For details, see *id.* at 4.

[115]Cœuré, *supra* note 53.

[116]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[117]For a comprehensive analysis of the provisions of the GDPR in a cybersecurity context, see Simon Stokes, *Data Protection, Information Security, and Cloud Computing*, 163 Comp. Officer Bull. 1, 2–24 (2019).

[118]For a brief overview of the NIS Directive, see Markus Dürig & Matthias Fischer, *Cybersicherheit in kritischen Infrastrukturen*, 42 Datenschutz & Datensicherheit 209, 209–11 (2018); Ludmila Georgieva, *The First EU-Wide Legislation on Cybersecurity*, 6 Eur. Energy J. 62 (2016).

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

Directive is the only piece of EU legislation that has an exclusive focus on cybersecurity for network and information systems and applies across different sectors.[119] Based on Article 114 TFEU, the directive aims at developing a minimum level of cyber capability in all Member States, rather than at the EU level.

The NIS Directive takes account of the essential role in the functioning of economic and social life attributed to operators of essential services and digital service providers. Regarding the financial sector, the NIS Directive applies to credit institutions, operators of trading venues, and central counterparties, when designated as operators of essential services.[120] Provisions in sector-specific EU legal acts, which—directly or indirectly under the umbrella of operational risk—impose cybersecurity requirements on financial institutions, such as CRD IV, PSD2, and MiFID II, are *lex specialis* vis-à-vis the NIS Directive provided that they contain requirements that are at least equivalent in effect to the obligations laid down in the NIS Directive.[121]

i) Content

Under the NIS Directive, credit institutions concerned must "take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of [their] network and information systems."[122] In addition, they have to "take appropriate measures to prevent and minimize the impact of incidents affecting the security of the network and information systems … with a view to ensuring the continuity of those services."[123] "In order to promote convergent implementation [of these requirements], Member States shall, without imposing or discriminating in favor of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems."[124] Finally, credit institutions must "notify, without undue delay, the competent authority … of incidents having a significant impact on the continuity of the essential services they provide."[125]

With regard to similar reporting requirements in the United States, the private sector raised the concern that an obligation to notify cyber-incidents increases risks of civil liability, regulatory liability, or both and advocated for clearly defined liability protections.[126] The NIS Directive took up this concern and clarified, "notification shall not make the notifying party subject to increased liability."[127]

ii) Critical Assessment

The provisions of the NIS Directive are very broad and abstract.[128] While such an open formulation leaves room for credit institutions to react with flexibility to dynamically evolving cyber threats, it also leaves them with uncertainty as to the cybersecurity standards to implement,

[119]Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA, 2013 O.J. (L 218) 8 does not address the prevention of cybersecurity incidents, but primarily covers the approximation of criminal law of the Member States in the area of attacks against information systems.

[120]NIS Directive, *supra* note 5, at arts. 4(4), 5(2) in conjunction with Annex II.

[121]*Id.* at rec. 9, 13 and art. 1(7). *See also* Eur. Supervisory Auth., *supra* note 47, at 14.

[122]NIS Directive, *supra* note 5, at art. 14(1).

[123]*Id.* at art. 14(2).

[124]*Id.* at art. 19(1).

[125]*Id.* at art. 14(3).

[126]From the US perspective, see Ariana L. Johnson, *Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation*, 20 N.C. Banking Inst. 277, 297–98, 305–07 (2016). *See also* Etzioni, *supra* note 39, at 72–73.

[127]NIS Directive, *supra* note 5, at art. 14(3).

[128]*See, e.g.*, *Id.* at art. 14(1) (noting the obligation to "take appropriate and proportionate … measures" with regard to the "state of the art").

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

especially when there is more than one standard available. Not only does this mean that there is a conflict with the principle of legal certainty, but it also is cause for concern inasmuch as competent authorities have the competence to "issue binding instructions to the operators of essential services to remedy the deficiencies identified."[129]

What is more—and unlike the SIPS Regulation—the high-level provisions of the NIS Directive do not sufficiently ensure the implementation of all essential elements of an efficient cybersecurity regulatory framework. For example, operators of essential services are not explicitly required to implement regular testing, internal control mechanisms, or to ensure regular staff training and continuous learning. In addition, the NIS Directive provides only minimum harmonization.[130] Cybersecurity requirements for credit institutions can, therefore, still diverge significantly from one Member State to another, resulting in very different levels of protection and preparedness, entailing a risk of regulatory arbitrage.[131] This is particularly problematic in that mutual trust and reinforced cooperation can be built only on a level playing field, which a "minimum level" of requirements and engagement cannot achieve. Finally, law enforcement bodies play a very limited role in the directive, although collaboration between the different cybersecurity communities is of vital importance.[132]

b) Cyber-Incident Reporting Framework

In 2017, the ECB published a cyber-incident reporting framework that applies to all banks under the direct supervision of the ECB and, therefore, to all significant institutions from the nineteen euro-area countries. Under this framework, banks are required to report significant cyber-incidents to the ECB as soon as they detect them. In Member States where such an incident reporting process was already in place, banks will continue to report incidents to the national supervisors, who will then forward them to the ECB.[133]

c) CRD IV, CRR, PSD2, and MiFID II

i) CRD IV and CRR

Pursuant to the CRD IV,[134] credit institutions shall "implement policies and processes to evaluate and manage the exposure to operational risk,"[135] put in place "contingency and business continuity plans,"[136] and "shall have robust governance arrangements" as well as "adequate internal control mechanisms."[137] Although these provisions do not explicitly reference cybersecurity but address operational risk in general, the management of cyber risks is broadly expected to be covered by these terms. To supplement the provisions of CRD IV, the EBA has issued a set of guidelines,[138] including a specific guideline on outsourcing arrangements.[139]

[129]*Id.* at art. 15(3). *See also* the criticism expressed by LEISTERER, *supra* note 55, at 78.

[130]NIS Directive, *supra* note 5, at art. 3.

[131]Moreover, Member States are free to decide whether they apply the requirements of the NIS Directive only to credit institutions, operators of trading venues and central counterparties, as stipulated by the NIS Directive as a minimum requirement, or also to other actors in the financial sector.

[132]Carrapico & Barrinha, *supra* note 11, at 1266.

[133]FSB, *supra* note 38, at 70.

[134]Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on Access to the Activity of Credit Institutions and the Prudential Supervision of Credit Institutions and Investment Firms, Amending Directive 2002/87/EC and Repealing Directives 2006/48/EC and 2006/49/EC, 2013 O.J. (L 176) 338 [hereinafter CRD IV]. CRD IV has been based on TFEU art. 53(1).

[135]*Id.* at art. 85(1).

[136]*Id.* at art. 85(2).

[137]*Id.* at art. 74(1).

[138]European Banking Authority (EBA), Guidelines on Internal Governance, EBA/GL/2017/11 (Mar. 21, 2018); European Banking Authority (EBA), Guidelines on ICT Risk Assessment Under the Supervisory Review and Evaluation Process (SREP), EBA/GL/2017/05 (May 11, 2017).

[139]European Banking Authority (EBA), Guidelines on Outsourcing Arrangements, EBA/GL/2019/02 (Feb. 25, 2019).

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

The Capital Requirements Regulation (CRR)[140] contains relevant provisions in Articles 288, 320–322, and 368.[141]

ii) PSD2

In their capacity as payment services providers, credit institutions must observe the requirements of PSD2.[142] With regard to third-party risks, the directive stipulates, "outsourcing of important operational functions, including IT systems, shall not be undertaken in such way as to impair materially the quality of the payment institution's internal control."[143] Moreover, PSD2 requires payment service providers that apply for authorization as a payment institution to "indicate how they ensure a high level of technical security and data protection … for the software and IT systems …."[144] Apart from these explicit references to cybersecurity, the management of cyber risks is only indirectly covered by provisions on the management of operational and security risks of a payment services provider,[145] and on notification requirements in case of a major operational or security incident.[146] In order to supplement the provisions of the PSD2, the EBA, in close cooperation with the ECB, has issued a set of guidelines.[147] In addition, the "EBA shall promote cooperation, including the sharing of information, in the area of operational and security risks associated with payment services among the competent authorities, and between the competent authorities and the ECB and, where relevant, the ENISA."[148]

iii) MiFID II

When providing one or more investment services, performing investment activities, or both, credit institutions must also observe certain provisions of MiFID II,[149] including Article 16 MiFID II.[150] Under this article, a credit institution "shall employ appropriate and proportionate systems, resources, and procedures"[151] and must establish "internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for information processing systems."[152] Moreover, "sound security mechanisms [must be] in place to … minimize the risk of data corruption and unauthorized access and to prevent information leakage."[153]

[140]Regulation (EU) No. 575/2013 of the European Parliament and of the Council of 26 June 2013 on Prudential Requirements for Credit Institutions and Investment Firms and Amending Regulation (EU) No. 648/2012, 2013 O.J. (L 176) 1 [hereinafter CRR]. CRR has been based on TFEU art. 114.

[141]For more details, refer to Eur. Supervisory Auth., *supra* note 47, at 20.

[142]Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and Repealing Directive 2007/64/EC, 2015 O.J. (L 337) 35 [hereinafter PSD2]. PSD2 has been based on TFEU art. 114.

[143]*Id.* at art. 19(6), subpara. 2.

[144]*Id.* at art. 5(1), subpara. 3.

[145]*Id.* at art. 95.

[146]*Id.* at art. 96.

[147]European Banking Authority (EBA), EBA Guidelines on ICT and Security Risk Management, EBA/GL/2019/04 (Nov. 28, 2019). The guidelines have been based on PSD2 arts. 95(3), 96(3). Where requested to do so by the Commission, the EBA shall also develop draft regulatory technical standards on the criteria and on the conditions for establishment and monitoring of security measures, PSD2 art. 95(4).

[148]PSD2 art. 95(5).

[149]Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on Markets in Financial Instruments and Amending Directive 2002/92/EC and Directive 2011/61/EU, 2014 O.J. (L 173) 349 [hereinafter MiFID II]. MiFID II has been based on TFEU art. 53(1).

[150]*Id.* at art. 1(3)(a).

[151]*Id.* at art. 16(4).

[152]*Id.* at art. 16(5), subpara. 2.

[153]*Id.* at art. 16(5), subpara. 3.

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

MiFID II also addresses third party risk management. In this regard, a credit institution "shall ensure, when relying on a third party for the performance of operational functions … that it takes reasonable steps to avoid undue additional operational risk."[154] In order to specify the concrete requirements in this context, the Commission has adopted a delegated regulation.[155]

2.2 Overall Assessment

Too many cooks spoil the broth. This wisdom also applies to cybersecurity regulation for credit institutions. The regulatory landscape in this area is composed of various legal instruments of both legally binding and non-binding quality, which have been adopted by many different regulators. Fragmentation of requirements for credit institutions across the NIS Directive, CRD IV, PSD2, and MiFID II leads to a lack of clarity. Overlapping or duplicative requirements entail a risk of inconsistency. This is problematic because legal clarity and consistency are necessary to ensure a level playing field for financial institutions. There also is a high degree of fragmentation in the level of detail, specificity, and terminology of the relevant provisions.[156] This can adversely affect credit institutions that are subject to more than one of the aforementioned legal acts.

As in the NIS Directive, the relevant provisions of CRD IV, CRR, PSD2, and MiFID II are very high level. In addition, most of them are not explicit on cybersecurity, but only address the management of the general operational risk of a credit institution. More specifically, cybersecurity-related requirements are laid down in only supplemental, non-binding guidelines. Preferably, cybersecurity should be regarded as an independent risk management category in need of more explicit, mandatory rules that ensure that every relevant entity is subject to specific cybersecurity requirements.

With regard to incident notification, many different reporting schemes exist at both the national and EU levels. Some of these schemes are governed by sectoral legislation, others by cross-sectoral legislation, such as the NIS Directive and the GDPR.[157] The schemes differ in scope, addressees, terminology, and requirements (for example, different timeframes). They also designate different recipients of the reported information. For some incidents, the frameworks overlap.[158] An additional source of complication stems from differences in reporting templates. This can become burdensome, especially in time-critical environments.[159]

Finally, there are no legally binding provisions[160] that specifically address third-party concentration risk.

III. EU Cybersecurity Governance Structures

European governance of cybersecurity is rather decentralized.[161] With regard to the EU public sector, relevant bodies can be assigned to the three different areas of cybersecurity: Network and information security, cybercrime, and cyber defense.

[154] *Id.* at art. 16(5), subpara. 1.

[155] *See* arts. 21, 23, 30–32 of the Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 Supplementing Directive 2014/65/EU of the European Parliament and of the Council as Regards Organizational Requirements and Operating Conditions for Investment Firms and Defined Terms for the Purposes of that Directive, 2017 O.J. (L 87) 1. The Regulation has been based on MiFID II arts. 16(12), 89.

[156] Eur. Supervisory Auth., *supra* note 47, at 7, 11.

[157] For an overview of some of the most important incident notification schemes at EU level, see *id.* at 24.

[158] *Id.* at 16.

[159] *Id.* at 17.

[160] The EBA Guidelines on Outsourcing Arrangements, *supra* note 139, briefly address outsourcing concentration risk.

[161] Carrapico & Barrinha, *supra* note 11, at 1261.

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

1. Network and Information Security

1.1 ENISA

With ENISA, the EU has a dedicated agency in the field of cybersecurity. ENISA, originally established in 2004, pursues mid and long-term objectives. It aims to raise awareness and assist the EU, Member States, and public and private stakeholders develop and improve cyber resilience and response capacities, including building of Computer Emergency Response Team (CERT) capacities. ENISA also organizes the pan-European cyber crisis exercise that simulates a crisis scenario caused by a large number of cybersecurity incidents.

With the entry into force of the EU Cybersecurity Act (ECA)[162] in June 2019, ENISA has been provided with a new permanent mandate, a reinforced role in cybersecurity with new tasks, and additional financial and human resources. Most importantly, ENISA will be responsible for the preparation of European cybersecurity certification schemes, which will serve as the basis for certification of ICT products, processes, and services. In addition, ENISA will continue to support the coordination of responses to large-scale cyber-attacks and crises, in cases where two or more Member States are concerned. Still, ENISA has no direct intervention powers.

1.2 CERT-EU, CSIRTs, Cooperation Group, CSIRTs Network and FIRST

The Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) deals with concrete information security incidents and cyber threats. However, for the time being, it provides its services only to EU institutions and has limited resources.[163]

Under the NIS Directive, each Member State shall set up a national Computer Security Incident Response Team (CSIRT) for handling risks and incidents[164] and must designate or establish authorities competent to monitor the NIS Directive's application as well as a single point of contact.[165] To date, respective national structures still diverge significantly in form, function, and equipment.

According to the NIS Directive, CERT-EU will become a member of the CSIRTs network, together with the national CSIRTs.[166] This CSIRTs network will promote the possibility of voluntary operational cooperation. In addition, a "Cooperation Group," composed of representatives of the Member States, the Commission, and ENISA, will provide strategic guidance to the CSIRTs network and shall also coordinate the exchange of best practices among the Member States.[167] Outside the scope of the NIS Directive, collaboration within the European CSIRT community takes place in the TF-CSIRT.[168]

Computer Emergency Response Teams do not only exist at the public level but are also set up in-house in private firms and organizations. The Forum of Incident Response and Security Teams (FIRST) brings together a variety of CERTs from governments and non-governmental organizations and businesses. FIRST aims to foster cooperation and coordination in incident prevention and to promote information and experience sharing concerning attacks and malware, while building professional relationships of trust.[169]

[162]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), 2019 O.J. (L 151) 15. The EU-wide certification system gives a strong competitive advantage to European products proven to be cybersecure and encourages cybersecurity by design in all processes, thereby increasing trust and security in products and services.

[163]EPSC, *supra* note 27, at 7.

[164]NIS Directive, *supra* note 5, at art. 9. For concerns related to data protection in this context see generally Kurt Einzinger & Florian Skopik, *Über die datenschutzrechtliche Problematik in CERTs/CSIRTs-Netzwerken*, 41 DATENSCHUTZ & DATENSICHERHEIT 572 (2017).

[165]NIS Directive, *supra* note 5, at art. 8.

[166]*Id.* at art. 12(2).

[167]*Id.* at art. 11. The Cooperation Group established under the NIS Directive is not to be confused with the EGC Group (*see infra* text accompanying note 178).

[168]For more information on TF-CSIRT, visit https://tf-csirt.org/tf-csirt/.

[169]Bendiek & Porter, *supra* note 13, at 171.

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

1.3 Actors in the Financial Sector in Particular

With regard to cybersecurity in the financial sector, the European Supervisory Authorities (ESAs), the ECB, the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB), and the European Financial Institutes Information Sharing and Analysis Centre (European FI-ISAC) stand out. The ESAs and the ECB are involved in the daily supervision of financial market participants, which also concerns cybersecurity, and they are active in the field of rulemaking, issuing binding rules and soft law. The ECRB is a forum for strategic discussions, collaboration, and sharing of best practices between pan-European FMIs, their critical service providers, and public authorities.[170] Facilitated by the ECB, it has no formal powers to impose binding measures and does not make supervisory judgments.[171] With a similar focus, the mission of the European FI-ISAC is to exchange information on ICT related topics, including cybercriminal activity affecting the financial community, vulnerabilities, technology trends, incidents, and case studies.[172] The European FI-ISAC is composed of country representatives from the financial sector, CSIRTs, and Law Enforcement Agencies. The equivalent of the European FI-ISAC at the global level is the Financial Services Information Sharing and Analysis Center (FS-ISAC).

2. Cybercrime: European Cybercrime Centre (EC3)

The European Cybercrime Centre (EC3) at Europol provides important operational support and training to the Member States and has become the first hub for expertise on cybercrime operations. In this regard, the EC3 is a victim of its own success. Given the importance and recognition it has gained since its creation in 2013, it is already understaffed and needs to see significant enforcement of resources.[173]

3. Cyber Defense: European Defence Agency (EDA) and EU Military Staff

The role of the EU in cyber defense is largely limited to an advisory function, leaving the operational and strategic realities of defense to the Member States.[174] The European Defence Agency (EDA) supports the capability development in cyber defense in the Member States and encourages greater cooperation in this field. The EU Military Staff brings cyber expertise to military strategic planning in the Common Security and Defence Policy (CSDP) military operations and missions.[175]

4. Assessment of the Governance Structures

The EU's current approach to cybersecurity is siloed within various institutions, actors, and initiatives, and it is characterized by a lack of clearly delineated areas of responsibility.[176] There are coordination problems between and within these silos. Certain capabilities and mandates are duplicates. Interaction between the different cyber-communities proves difficult for technical,

[170] *See generally Euro Cyber Resilience Board for pan-European Financial Infrastructures*, EUR. CENTRAL BANK, https://www.ecb.europa.eu/paym/groups/euro-cyber-board/html/index.en.html (last visited Jan. 21, 2020).

[171] Benoît Cœuré, *Euro Cyber Resilience Board for pan-European Financial Infrastructures*, EUR. CENTRAL BANK, (Mar. 9, 2018), https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180309_1.en.html (Introductory remarks at the first meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures).

[172] *See generally European Financial Institutes—Information Sharing and Analysis Centre, A Public-Private Partnership*, ENISA, https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/finance/european-fi-isac-a-public-private-partnership (last visited Jan. 21, 2020).

[173] Pupillo, Griffith, Blockmans & Renda, *supra* note 36, at 43; EPSC, *supra* note 27, at 7. For a comprehensive analysis of EU cybercrime governance, see George Christou, *The Challenges of Cybercrime Governance in the European Union*, 19 EUR. POL. & SOC'Y 355 (2018).

[174] Pupillo, Griffith, Blockmans & Renda, *supra* note 36, at 42.

[175] EPSC, *supra* note 27, at 7.

[176] *See also* Carrapico & Barrinha, *supra* note 11, at 1264.

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

legal, and cultural reasons. This puts major limitations to the fight against cyber-attacks because it cannot be solved by looking only at the contaminated devices, as the CERT community would, but can only be fully understood by observing the big picture, as only police and law enforcement can.

At the Member State level, CERT structures diverge significantly in form and function.[177] The NIS Directive has changed little in this regard because it only provides for minimum harmonization and has a limited scope of application. Different levels of cyber maturity and preparedness are another hurdle to the fight against cyber-attacks. Not only is it difficult to achieve smooth cooperation between the different cyber-communities, but even at the level of a specific community, like the CERT community, it proves delicate to enforce cross-border exchange and cooperation among different national structures.

Until the establishment of the CSIRTs network and the Cooperation Group, cooperation among governmental CERTs took place only in the European Government CERTs group (EGC group), an informal association of governmental CERTs in Europe composed only of the authorities of the most capable states,[178] and the Central European Cyber Security Platform (CECSP).[179] In the past, both groups were reluctant when it came to widening their circle. The very functioning of everyday life and business is at stake here, and cyber threats do not know a geographical dimension. States, therefore, trusted and wanted to open up to systems that are only as safe as their own; at the same time, however, it is also the reason why cross-border cooperation is indispensable.

It is at least questionable whether the CSIRTs network and the Cooperation Group will change things up in this regard because the underlying problems—notably, heterogeneity in the level of maturity—remain largely the same, and cooperation within the new structures is still voluntary to a large extent.

F. Reform Perspectives for Cybersecurity Regulation and Governance in the Financial Sector

Owing to their transnational nature, a global answer to cyber threats is often advocated.[180] Therefore, it is not surprising that the idea to adopt an international regulatory framework on cybersecurity in the financial sector has already been brought forward.[181] In order to ensure implementation and to create a level playing field, such a framework would need to be legally binding. Currently, however, the conclusion of an international treaty or a similar, binding *global* agreement in a highly technical and sensible area such as cybersecurity does not seem very likely.[182] Yet, at the EU level, the adoption of a legally binding regulatory framework on cybersecurity in the financial sector is conceivable. In the most general sense, the EU's strength is to facilitate coordination and cooperation between the Member States; harmonize policies and agendas; and encourage the pooling or aggregation of resources, capabilities, and responsibilities.[183]

[177]Pupillo, Griffith, Blockmans & Renda, *supra* note 36, at 39; EPSC, *supra* note 27, at 7.

[178]Members are: Austria, Belgium, Denmark, Finland, France, Germany, Netherlands, Norway, Spain, Sweden, Switzerland, UK, and the CERT-EU.

[179]Members are the Visegrád Countries (Czech Republic, Hungary, Poland, Slovakia) and Austria.

[180]*See, e.g.*, V. Gerard Comizio, Behnam Dayanim & Laura Bain, *Cybersecurity as a Global Concern in Need of Global Solutions: An Overview of Financial Regulatory Developments in 2015*, 17 J. Inv. Compliance 101, 102 (2016); Iulian F. Popa, *EU Cyberspace Governance: Which Way Forward*, 5 Res. & Sci. Today 115, 122 (2013); Cœuré, *supra* note 53; EPSC, *supra* note 27, at 14.

[181]*See, e.g.*, Ingolf Pernice, *Global Cybersecurity Governance: A Constitutionalist Analysis*, 7 Glob. Const. 112, 115, 132–36 (2018).

[182]Similarly, with regard to financial regulation at global level in general, see Bachmann, *supra* note 82, at 3, 21.

[183]Pupillo, Griffith, Blockmans & Renda, *supra* note 36, at 33. *See generally* Myriam D. Cavelty, *Europe's Cyber-Power*, 19 Eur. Pol. & Soc'y 304 (2018).

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

A potential reform at the EU-level could start with the adoption of a European Single Cybersecurity Rulebook for the Financial Sector. Better cooperation and information sharing within the private sector, between the private and the public sector, and among public authorities would also need to be addressed. In this context, the creation of a European Cybersecurity Platform could be considered.

I. Adoption of a European Single Cybersecurity Rulebook for the Financial Sector

In order to address the current fragmented and heterogeneous regulatory landscape for cybersecurity in the financial sector, provide legal certainty, establish a level playing field among financial institutions, and ensure a comparable level of cyber resilience maturity of financial sector participants, a European Single Cybersecurity Rulebook for the Financial Sector could be adopted.

Based on Article 114(1) TFEU, the Single Rulebook would establish specific and coherent cybersecurity requirements and use consistent terminology. It would apply to every financial participant, regardless of its significance or size.[184] As its name implies, the Cybersecurity Rulebook would address cybersecurity as an independent risk management category and take the form of a regulation or a directive providing for full harmonization.

Admittedly, having one solitary rulebook for the broad range of financial institutions, of different sizes, would be difficult. It might end up being very high level, leading to supervisors taking very different approaches to assessing compliance with its provisions. The proposed Single Rulebook is, therefore, not to be understood as a "one-size-fits-all" solution, but rather as a framework of reference providing common cybersecurity pillars for every subsector of the financial sector.

1. Substantive Provisions

1.1 Content

With regard to its substantive provisions, the Single Cybersecurity Rulebook would cover all vital elements of an effective cybersecurity regulatory framework, including, but not limited to, the prevention and detection of, the response to, and the recovery from a cyber-attack. Article 15(4) SIPS Regulation and Article 14(1) to (3) NIS Directive could serve as an example in this regard but would need to be complemented by more specific provisions and requirements. The power to adopt technical specifications would be delegated to the Commission, which would be supported by ENISA and the ESAs.

a) Penetration-Testing and Red Teaming

Specific provisions on cross-border and cross-authority system penetration testing and red teaming could be built on already existing instruments such as the ECB's TIBER EU-Framework for Threat Intelligence-based Ethical Red Teaming[185] or the G7 CEG 2018 Fundamental Elements for Threat-Led Penetration Testing.[186]

b) Management of Third Party Cyber Risks

The management of third-party cyber risks, especially regarding interconnections with cloud services providers and related concentration risks, should also be addressed in more specific and legally binding rules. These could be built on the G7 CEG 2018 Fundamental Elements for

[184] *See supra* text accompanying notes 44–45.

[185] Eur. Cent. Bank, TIBER-EU Framework: How to Implement the European Framework for Threat Intelligence-Based Ethical Red Teaming (2018), https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf.

[186] G7 Conference, *supra* note 93.

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

Third Party Cyber Risk Management in the Financial Sector.[187] If the adoption of outsourcing guidelines or enabling supervisor's access onsite proves insufficient to mitigate cyber risks stemming from third-party interconnections, direct supervision of third-parties would be a conceivable solution.

c) Consistent Incident Notification Schemes

Moreover, consistent incident notification requirements should be introduced for all financial sector participants.[188] These requirements should ensure that the same entity is not subject to different reporting timeframes or must use different reporting templates. Requirements should also take into consideration suitable criteria for incidents to be reported, in addition to specifying the recipients of incident reports.[189] Finally, the reporting of not only incidents but also of tactical and strategic information should be considered, but remain voluntary.

1.2 Regulatory Technique

With regard to the regulatory technique to be used in the Rulebook, the legislator would be required to build in flexibility into regulation in order to promote the agility and adaptability of businesses and institutions,[190] thereby enabling them to continually improve themselves against an ever-changing threat landscape.[191] In order to achieve greater flexibility, the legislator can make use of different tools.

a) Binding Objectives and Focus on Outcomes

Probably the most important tool to enhance flexibility and to promote agility and adaptability through regulation is to focus on outcomes. To this end, principle-based regulation defines binding objectives which set a target and the criteria to be followed to achieve compliance, instead of prescribing the exact mechanisms by which compliance is obtained.[192] Principle-based regulation induces the development of new, cost-effective methods and techniques to comply. What is more, setting targets without prescribing the methods avoids the risk of creating lock-ins. Lock-ins may occur if the regulatory requirements refer to a specific technique to meet a target, leaving no room for other techniques or methods. By contrast, rule-based regulation stipulates not only the target but also how to meet the target. Such an approach requires the regulator to provide a very specific set of rules. Rule-based regulation is usually easier to control and enforce by the authorities, precisely because it is rather inflexible and standardized. But it hardly sets incentives for companies to develop their own approaches to meet the target.

The principle-based approach aims to counter the box-ticking mentality often reproached to rule-based regulatory systems. Risk regulation—like cybersecurity[193]—cannot fully be conceived *ex ante* but needs regular and speedy adjustments *ex post*. Under the principles-based approach, regulated entities will have increased flexibility in how they deliver the outcomes that the regulator requires, and many will find a closer fit between meeting their business objectives and meeting regulatory requirements.[194] Wherever possible and appropriate, the provisions of the Rulebook should, therefore, be principle-based.

[187] G7 Conference, *supra* note 92.

[188] *See also* Cœuré, *supra* note 53.

[189] Eur. Supervisory Auth., *supra* note 47, at 16.

[190] This is also a recommendation formulated by Healey, Mosser, Rosen & Tache, *supra* note 7, at 13 ("Harmonize international regulations that foster resilience to cyber attacks and mitigate risk in the event of an attack. This regulatory and supervisory approach should have enough elasticity to evolve with technological changes and adversary sophistication.").

[191] *See supra* text accompanying notes 38–40.

[192] Pelkmans & Renda, *supra* note 39, at 5.

[193] See Fahey, *supra* note 11, at 53–55, 58–59.

[194] Ben Wilson, *What Are the Benefits of Principles-Based Regulation?*, Grovelands Fin. Serv. News, (June 10, 2018), https://grovelands.co.uk/financial-services-news/why-we-need-principles-based-regulation/. *See also* Jan Dalhuisen, 3 Transnational Comparative, Commercial, Financial and Trade Law 558–60 (7th ed. 2019).

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

b) Sunset Clauses

Sunset clauses are a way to react to a rapidly changing world that the legislator often has difficulties keeping up with. Sunset clauses can be defined as legal or regulatory clauses that shall be extinguished after a fixed period, except if the renewal of the clause is requested.[195] Sunset clauses bear a resemblance to experimental legislation because they enable the legislator or regulator to "try out" new regulatory approaches. This can be useful in a situation of great uncertainty and lack of information. When little is known about a situation, a temporary legislative measure can be a better option than no legislative adjustment to the situation. What is more, sunset clauses may ease the decision of the legislator because the decision is easily extinguished. Lawmakers can use sunset clauses to gather information and experience. For these reasons, sunset clauses can encourage quicker legislative or regulative changes in dynamic fields or under uncertain circumstances.

2. Supervisory Structure

At the supervisory level, current structures would remain largely unchanged. In particular, all European and national supervisors currently responsible for the financial supervision of a certain subsector or parts of it would continue to supervise that subsector, including oversight of cybersecurity requirements. They would, however, apply the new Cybersecurity Rulebook. As opposed to a conceivable "single cybersecurity supervisor" for the entire financial sector, sector supervisors have specific knowledge of the particularities of their area and the entities they supervise. But they might not all be cybersecurity experts. In their daily supervision, they would, therefore, be advised and supported by both European and national cybersecurity competence centers to be composed of experts and staff with a dedicated IT background and an in-depth knowledge of cybersecurity. Regarding their institutional structure, the competence centers could be set-up within existing organizations with a similar focus, like ENISA or EU and governmental CERTs, or as an independent organization.

II. Reinforcement of Cooperation and Information Sharing

Within the EU, considerable rhetorical emphasis is put on the development of a common approach to cybersecurity based, among others, on the enhancement of cooperation and information sharing among actors and policies.[196] At its current state, however, the EU is insufficiently prepared. The same information is usually passed through different sources; various groups process information and act in parallel. Overall, coordination must be improved, and existing resources at all levels must be pooled.[197]

1. Within the Private Sector

Within the private sector, cooperation and information sharing is currently voluntary. There are limited incentives to reveal cyber-incidents or related information to other firms. Apart from competition concerns, many firms do not have the trust of all other players and will be reluctant to share sensitive information.[198] Legal constraints, such as confidentiality, banking secrecy, and data protection, further inhibit information sharing. In order to encourage cooperation and

[195]Sofia Ranchordás, Constitutional Sunsets and Experimental Legislation 52 (2014).

[196]Carrapico & Barrinha, *supra* note 11, at 1261.

[197]According to Sales, *supra* note 2, at 1546–47, public health law could serve as a regulatory example for more efficient information sharing in the cybersecurity field ("Like health care providers who diagnose and then report their patients' infectious diseases, firms could be tasked with monitoring their systems for vulnerabilities and intrusions, then reporting their findings and the countermeasures they have implemented to designated recipients.").

[198]*See also* Sales, *supra* note 2, at 1549.

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

information sharing—and having recourse to the concept of "*Auffangverantwortung*"[199]—regulators could provide a legal framework that guarantees the confidentiality of firm-specific information, for example, through the anonymization or aggregation of information shared. Such measures would also reduce concerns of increasing insurance premiums or adverse effects on an institution's reputation or competitive position. Exemptions from contractual, tort, and regulatory liability regimes, such as the one stemming from the GDPR, could be discussed as well. Finally, a European Cybersecurity Platform with different sub-platforms could be set up to allow smaller groups of firms to share information based on mutual trust freely. This will need to be a gradual process. State intervention and mandatory information sharing within the private sector should be considered only if the voluntary collaborative approach led to obvious shortcomings.

2. Between the Private Sector and Public Authorities

Private institutions and public authorities exchange information through several mandatory incident notification schemes and cooperate on a voluntary basis in public-private partnerships and networks such as the ECRB and the European FI-ISAC. While private firms typically know more than outsiders about the architecture of their systems and its potential weaknesses, the government, via their intelligence services, typically knows more than private firms about cyber threats stemming from foreign governments.[200] Looking ahead, there needs to be a mind-shift to move beyond incident reporting towards also sharing *ex ante* operational, tactical, and strategical threat intelligence.[201] Such a mind-shift could be realized through the creation of a European Cybersecurity Platform.

3. At the Public Level

At the public level, organizations like ENISA, the EGC group, the CECSP, or the CSIRTs network and the Cooperation Group have a mandate to facilitate cross-border and cross-sectoral cooperation and information sharing among national and European authorities. Information to be shared should include cyber-incidents and operational, tactical, and strategical threat intelligence. One major obstacle to information sharing at the public level is, however, that the Member States often consider these kinds of information confidential and do not want to share it for national security reasons. In order to enhance Europe's position as a world leader in the digital economy and to create a Digital Single Market for financial services and goods, they must open up in this regard eventually.

Finally, the reporting of cyber-incidents affecting civil society and individuals must be facilitated in order to have sufficient awareness of the cybersecurity landscape in Europe and of the emergence of new vulnerabilities and threats. Member States should be encouraged to establish national helpdesks, for example, a national cybersecurity officer.

III. Integrating the Financial Sector in a European Cybersecurity Platform

To this end, a common EU body for sharing intelligence, analyzing cyber threats, and providing strategic reports could be established.[202] Its task would be to "connect the dots" in the currently fragmented institutional cybersecurity infrastructure within the EU and its Member States on the one hand, and public authorities and the private sector on the other. Taking account of the security prerogative of Member States, the Platform would not assume executive competences.

[199] *See supra* text accompanying notes 55–57.

[200] Sales, *supra* note 2, at 1518.

[201] ENISA, *supra* note 43, at 37.

[202] *See also* EPSC, *supra* note 27, at 9–11. For a similar, but farther-reaching set of proposals in the area of cyber defense, see Pupillo, Griffith, Blockmans & Renda, *supra* note 36, at 47–62.

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

1. Rationale

As a starting point, an efficient response to cyber-attacks requires the development of strategic capabilities at the EU level, such as expertise, information checking and analysis, and scenario and threat assessment. At the operational level, this would allow to close information gaps of national law enforcement authorities, providing them with the necessary information to tackle threats and prevent attacks. On this basis, a wide range of operational responsibilities, from incident response and investigation support to coordination and frontline operations, could be developed at Member States level by public authorities and in close cooperation with private actors.

The idea is thus to task a body, which is not intended to replace but to support the relevant actors in the Member States and at the European level. For instance, support would mean providing a hub to share information and expertise between national cybersecurity services across all Member States, and compiling "overall assessments" on cyber threats and changing modus operandi of cyber-attacks from a European perspective. The *National Cyber Security Centre* in the United Kingdom (NCSC UK) or the *Nationaal Cyber Security Centrum* in the Netherlands (NCSC NL) could serve as an example in this regard.

At the European level, this task could be implemented by a European Cybersecurity Platform. Such a platform could merge information deriving from the relevant actors active in all three areas of cybersecurity in order to depict a "European picture of cybersecurity." On this basis, it could provide a platform to jointly elaborate holistic responses to all kind of cyber-attacks within the EU. Such an independent strategic analysis and assessment of collectively shared information may contribute to creating a joint European perception of threats and challenges in the field of cybersecurity and provide common situational awareness among national authorities and the private sector.

Member States and private actors are far more likely to seek bilateral cooperation with like-minded actors. For this reason, it is highly important to establish a constant platform where different ideas on how to counter cyber-attacks can be discussed with the aim of defining common approaches to cybersecurity. In this context, the European Cybersecurity Platform's analysis and strategic reports may deliver the necessary evidence for a constructive discussion. Functioning as a type of intermediary between the relevant actors, the Platform would rapidly gain experience in synchronizing preventive and repressive policies and guaranteeing that authorities complement each other instead of operating in parallel.

2. Operational Tasks

At the operational level, the European Cybersecurity Platform could make sure that national law enforcement authorities are provided with joint operational expertise. Based on the information provided, national authorities could adapt their investigative strategies as well as their preventive measures and could increase the effectiveness of their work. In this regard, Joint Investigation Teams could provide a ready-made framework for cooperation between national law enforcement authorities to implement operational measures.

The task of "connecting the dots" could be fulfilled gradually. As a first step and absolute precondition, the European Cybersecurity Platform would have to receive information held by EU actors as well as public and private actors at the national level. Such information would have then to be evaluated by the Platform in order to issue preventive "overall assessments" of cyber threats within the EU and to provide national authorities with realistic appraisals of situational developments and strategic recommendations. Additionally, the Platform would have to provide a framework for pooling this information among national authorities and EU bodies and could potentially accompany the implementation of the information it generated on the ground.

Privacy and competition-related concerns in the context of information exchange could be alleviated, at least to some extent, through the distribution of summary or aggregated data.

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press

Article 83(1) EMIR,[203] according to which "no confidential information … shall be divulged to any person or authority, except in summary or aggregate form," could serve as an example in this regard.[204]

3. Organizational Structure

The Platform would be composed of the head of ENISA, the head of the EU Intelligence and Situation Centre (INTCEN), a high representative from the Commission—for example a European Cybersecurity Coordinator working under the authority of its President or the Commissioner for the Security Union—[205] a representative of the CSIRTs network and the Cooperation Group and the representatives of different communities—like the financial sector—organized in specific sub-platforms.

It would be assisted by a small secretariat, composed of staff seconded from the relevant services of the Member States, from the Commission, and from the participating agencies. The Platform would meet once a month and issue monthly reports on connecting the dots that would bring together intelligence and operational expertise and knowledge.

At a certain point, however, the Platform could become too limited in its capacity and could make judicial and parliamentary review more difficult, which is of relevance particularly in a context where fundamental rights are at stake. Therefore, it is of utmost importance to guarantee efficient forms of accountability and judicial review. For that reason, in due course, the Platform could evolve into an independent body, such as an agency.

G. Conclusion

Cybersecurity in the financial sector is a dynamic and evolving policy field with unique challenges and specific characteristics. Among these characteristics, the strong involvement of private stakeholders in the rulemaking process stands out. This is all the more remarkable because the involvement of private parties in a security-related policy field is rather unusual. It is, however, of considerable benefit as long as it is guided by a clear legal framework.

In our modern society, only digital security and resilience will enable businesses to fully benefit from the value of data and the new information technology more generally. The EU, assuming its role as an important cybersecurity actor and recognizing the importance of cybersecurity regulation for the creation of a Digital Single Market for financial services and the resilience of the Banking and Capital Markets Union, has adopted different pieces of cybersecurity legislation which largely benefitted from previous work of private standard setters. While this was an important first step to improve cybersecurity in the financial sector, the Article has shown that the current EU regulatory landscape for cybersecurity, including overall governance structures, still has considerable weaknesses. In order to address these weaknesses, this Article put forward the adoption of a Single Rulebook for Cybersecurity in the Financial Sector and the creation of a European Cybersecurity Platform.

[203]Regulation (EU) No. 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC Derivatives, Central Counterparties and Trade Repositories, 2012 O.J. (L 201) 1.

[204]Similarly, NIS Directive, *supra* note 5, at rec. 40 stipulates, "information on incidents should be provided in an aggregated form at Union level."

[205]The tasks and responsibilities of the European Cybersecurity Coordinator could mirror those of the EU-Counter Terrorism Coordinator. Amongst others, they would include the presentation of policy recommendations, monitoring the implementation of existing strategy and regulation, and communication with non-EU states.

Cite this article: Calliess C, Baumgarten A (2020). Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective. *German Law Journal* **21**, 1149–1179. https://doi.org/10.1017/glj.2020.67

https://doi.org/10.1017/glj.2020.67 Published online by Cambridge University Press