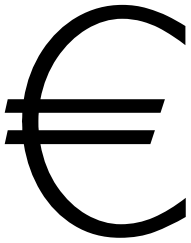


Reinforcing Financial Cybersecurity in the Eurozone

Editors and Lead Writers: Irene Velicer and Anwaar Ali

Writers: Nat Amos, Abi Crook, Hazel Ng, and Levinson Tan

The Wilberforce Society
Cambridge, UK
www.thewilberforcesociety.co.uk
December 2020

ACKNOWLEDGMENTS

Many thanks are due to Dr Andre Barrinha, Dr Jennifer Cobbe, Prof Jon Crowcroft, Dr Maria Demertzis, Mr Hazem Danny Al Nakib, Mr Sam Richardson, Prof Waltraud Schelkle, and Prof Paul Timmers for their generous time and comments.

We also thank the policy liaisons and administrative teams at The Wilberforce Society and European Horizons for their unfailing support throughout the disruptions caused by Covid-19.

IRENE VELICER AND ANWAAR ALI
EDITORS

ABSTRACT

Policy makers and policy researchers are paying increasing attention to financial cybersecurity in the Eurozone. The cross-border nature of cyberattacks and their effect on integrated financial networks are particular causes of concern. Although significant strides in policy are being made, European financial cybersecurity still faces a number of challenges. This paper considers how to reinforce recent measures by considering how to further mitigate fragmented approaches to cybersecurity, the possibility of cyber-induced financial risk, and the technological and regulatory challenges posed by emerging financial technologies. This paper's approach to reinforcement includes the harmonisation and streamlining of several relevant cybersecurity frameworks as well as the strengthening of resilience against the financial implications of cyber-induced instability.

The paper puts forward suggestions regarding the EU-level cyber hub idea, third-party+ oversight, and vulnerability disclosure. It also looks to improve cooperation between regulators and fintech developers through greater use of the regulatory sandboxing technique as well as through more frequent review of cybersecurity regulations in light of emerging technologies. In addition, the paper considers some of the issues posed by the exclusion of cyber warfare and cyber terrorism from many insurance policies and how to mitigate the effects of cyber-induced systemic instability. In doing so, the paper also puts forward suggestions on emergency funding for handling and mitigating cyber incidents (particularly cyber warfare and cyber terrorism).

N.B.

This paper was principally researched and written in the first half of 2020. With its completion having been extended by the Covid-19 pandemic, final revisions have sought to take account of the new EU Cybersecurity Strategy and the EU Commission's fall/winter 2020 proposals for financial 'digital operational resilience', markets in crypto-assets, DLT market infrastructures, and NIS II.

TABLE OF CONTENTS

ABBREVIATIONS

BIP: Bitcoin Improvement Proposals
CEF: Connecting Europe Facility
CEPS: Centre for European Policy Studies
CERT: Computer Emergency Response Team
CISA: Cybersecurity and Infrastructure Security Agency
CSIIF: Cyber Skills Immediate Impact Fund
CSIRT: Computer Security Incident Response Team
CVD: Coordinated Vulnerability Disclosure
DAO: Decentralized Authority Organization
DLT: Distributed Ledger Techology
DDoS: Distributed Denial of Service
DPA: Data Protection Authorities
EBA: European Banking Authority
EBOF: European Blockchain Observatory Forum
ECB: European Central Bank
ECRI: European Credit Research Institute
EDIRA: European Deposit Insurance and Resolution Authority
EIOPA: European Insurance and Occupational Pensions Authority
ENISA: European Union Agency for Cybersecurity
ESA: European Supervisory Authorities
ESM: European Stability Mechanism
ESMA: European Securities and Markets Authority
ESRB: European Systemic Risk Board
EU-CyCLONe: European Cyber Crises Liaison Organisation Network
FATF: Financial Action Task Force
FCA: Financial Conduct Authority
GDDP: Government Disclosure Decision Processes
GDPR: General Data Protection Regulation
INATBA: International Association for Trusted Blockchain Applications
JCU: Joint Cyber Unit
JRC: Joint Research Centre
NCSC: Nationaal Cyber Security Centrum
NHS: National Health Service
NIS Directive: Network and Information Security Directive
NIS II: Commission proposal for a revised NIS Directive
NSA: National Security Agency
OSS: Opensource Software
SIENA: Secure Information Exchange Network Application
SRF: Single Resolution Mechanism
SSM: Single Stability Mechanism
SWIFT: Society for Worldwide Interbank Financial Telecommunication
WEF: World Economic Forum

EXECUTIVE SUMMARY

A host of challenges face the Eurozone's financial cybersecurity and the cybersecurity of financial systems more generally. This paper engages with a number of these areas and offers suggestions for reinforcing the European financial system's resilience in a cyber age.

This paper's choice of topics is guided by three overlapping themes that the 2008-2012 financial crisis, the growth of cross-border cyber-attacks, and the rapidly changing cyber landscape have highlighted. The financial crisis brought the issue of systemic risk to the fore and cast a spotlight on the balance between harmonisation and decentralisation in the Eurozone. These are pressing issues that are relevant to cybersecurity. Financial integration in the Eurozone, persisting security fragmentation between EU member states, and the cross-border nature of many cyber-attacks make cyber-induced systemic risk more plausible than ever.[1] The increasing incorporation of emerging financial technologies (fintech) into mainstream financial infrastructures adds an additional dimension to these issues. It brings with it the perennial challenge of how to foster a happy marriage between innovation and regulation that will strengthen cybersecurity. In light of these developments, the themes that guide this paper's engagement with policy are the further mitigation of (1) remaining cybersecurity fragmentation, (2) cyber-induced systemic risk, and (3) tensions between cybersecurity regulations and emerging fintech in the Eurozone.

- The issue of **fragmentation** is fundamental to any analysis of European financial cybersecurity. Fragmentation here refers to diverse national, regional, and sectoral approaches to cybersecurity in the context of a highly integrated European financial system. Fragmentation can give rise to risks and frictions that have the potential to undermine the Eurozone's financial cybersecurity.[2]

- The 2008-2012 financial crisis has embedded the issue of systemic instability into contemporary financial consciousness. Given the growth of cross-border attacks, the integrated nature of the financial system, and persisting degrees of fragmentation in national security approaches, the possibility of **cyber-induced systemic instability** has received increasing attention. A February 2020 European Systemic Risk Board (ESRB)

[1] European Systemic Risk Board, *Systemic Cyber Risk* (2020).
[2] Maria Demertzis and Guntram Wolff, 'Hybrid and Cybersecurity Threats and the European Union's Financial System' (*Bruegel*, 2019) 7.

study marks a growing recognition that financial systems need to prepare for this eventuality.[3]

- Financial cybersecurity increasingly faces challenges posed by **emerging financial technologies**.[4] Embedding emerging technologies into financial systems increases system complexity. Junctures between systems in differently regulated jurisdictions and between legacy and emerging technologies can generate vulnerabilities.[5] Such vulnerabilities are possible sources of cyber-induced financial risk, including systemic risk.[6] Furthermore, some emerging fintech that have a growing place in the financial system have difficulty meeting cybersecurity standards.[7] Some have characteristics that challenge existing frameworks and definitions. Therefore, regulators and innovators need to further cooperate towards developing regulatory frameworks that are sensitive to the qualities of emerging fintech without compromising security.[8]

[3] European Systemic Risk Board, *Systemic Cyber Risk* (2020); Christine Lagarde, 'Remarks on the Occasion of Receiving the Grand Prix de l'Économie 2019 from Les Echos', (*European Central Bank*, 2020) <www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200205_1~cc8a8787f6.en.html> accessed 28 February 2020; cf. Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance: Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (Centre for European Policy Studies and European Credit Research Institute, 2018) 36-38; Maria Demertzis and Guntram Wolff, 'Hybrid and Cybersecurity Threats and the European Union's Financial System' (*Bruegel*, 2019) 6-11.

[4] In common parlance "fintech" can refer both to financial technologies themselves and to financial technology start-ups. This paper will use "fintech" in reference to the technologies and specify "fintech start-up" in reference to any companies.

[5] Claudia Ng, 'Regulating Fintech: Addressing Challenges in Cybersecurity and Data Privacy', (*Harvard Kennedy School,* 22 February 2018) <www.innovations.harvard.edu/blog/regulating-fintech-addressing-challenges-cybersecurity-and-data-privacy> accessed 6 June 2020.

[6] European Systemic Risk Board, *Systemic cyber risk* (2020) 13; Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions FinTech Action Plan: For a More Competitive and Innovative European Financial Sector [2018] COM/2018/0109 2.

[7] Michèle Finck, Blockchain and the General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law? (European Parliament, 2019) 52; Adrian Lawrence et al., 'Blockchain and Laws. Are they Compatible?—A White Paper Championed by Baker McKenzie in Collaboration with R3' (Baker McKenzie, 2017) 4-6; Claudio Lima, 'Developing Open and Interoperable DLT/Blockchain Standards' [2018] 51(11) IEEE Computer Society.

[8] Claudia Ng, 'Regulating Fintech: Addressing Challenges in Cybersecurity and Data Privacy', (*Harvard Kennedy School,* 22 February 2018) <www.innovations.harvard.edu/blog/regulating-fintech-addressing-challenges-cybersecurity-and-data-privacy> accessed 6 June 2020; Dan Panitz and Bruce Gordon, 'Balancing the Equation Between Technology and Effective Legal Project Management' (*Law.com: Corporate Counsel,* 6 March 2020) <https://www.law.com/corpcounsel/2020/03/06/balancing-the-equation-between-technology-and-effective-legal-project-management/?slreturn=20200810110120> accessed 10 September 2020.

Choice of policy areas within these themes:

In light of these three themes and their overlap, this paper **first** considers frameworks for reporting and sharing information about incidents and vulnerabilities. In a system where a cyber event can rapidly propagate security problems upstream and downstream, effective reporting and information sharing is crucial.[9] Therefore,

- This paper appraises existing proposals for an EU-level *cyber incident reporting hub* as well as methods for improving *coordinated vulnerability disclosure*, which can each facilitate information sharing.
- It also considers additional measures for reinforcing *third-party+ oversight* (i.e., that of third parties and their sub-contractors). Strong third-party+ oversight is important for information sharing and reporting mechanisms as well as wider system security.

Next, this paper considers how regulators and innovators can take a more harmonised and cooperative approach towards emerging fintech's relationship with regulation. Cooperation on reducing disjunction between regulation and emerging technologies can strengthen security standards, oversight, and incident reporting.[10] Such disjunctions (e.g., with respect to the identification of responsible actors in fintech like blockchain) can exacerbate interface vulnerabilities and pose problems for incident reporting and handling. In doing so, they have the potential to heighten cyber-induced systemic risk.[11] While the EU has taken initiative to improve the regulator-innovator relationship, more remains to be done.[12] Therefore,

---

[9] European Systemic Risk Board, *Systemic Cyber Risk* (2020) 3.

[10] Claudia Ng, 'Regulating Fintech: Addressing Challenges in Cybersecurity and Data Privacy', (*Harvard Kennedy School,* 22 February 2018) <www.innovations.harvard.edu/blog/regulating-fintech-addressing-challenges-cybersecurity-and-data-privacy> accessed 6 June 2020; Dan Panitz and Bruce Gordon, 'Balancing the Equation Between Technology and Effective Legal Project Management' (*Law.com: Corporate Counsel,* 6 March 2020) <https://www.law.com/corpcounsel/2020/03/06/balancing-the-equation-between-technology-and-effective-legal-project-management/?slreturn=20200810110120> accessed 10 September 2020; David Collingridge, *The Social Control of Technology* (Open University Press, 1981).

[11] 'Decentralised Financial Technologies: Report on Financial Stability, Regulatory and Governance Implications' (*Financial Stability Board,* 2019) 6-10; Claudia Ng, 'Regulating Fintech: Addressing Challenges in Cybersecurity and Data Privacy', (*Harvard Kennedy School,* 22 February 2018) <www.innovations.harvard.edu/blog/regulating-fintech-addressing-challenges-cybersecurity-and-data-privacy> accessed 6 June 2020.

[12] European Securities and Markets Authorities, European Banking Authority, European Insurance and Occupational Pensions Authority, 'Report—FinTech: Regulatory Sandboxes and Innovation Hubs' [2018] JC 74 3-6; 'Looking into the Crystal Ball: A Report on Emerging Technologies and Security Challenges' (*ENISA,* 2018) 5-6, 29-32; 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] OJ L 151 Art. 49 (3); 'ENISA Launches Public Consultation for First Candidate Cybersecurity Certification Scheme' (*ENISA*, 2 July 2020)

- This paper considers how to keep regulation and technologies in closer sync, particularly through improved cooperation between regulators and innovators. It looks at the periods of *regulatory review* and the extent of *regulatory sandboxing* in the EU.

- Of many relevant fintech, this paper looks at *blockchain*. This choice is motivated by the gradual uptake of decentralised fintech into mainstream financial systems and the difficulties they pose for existing regulatory frameworks.[13] Some of their characteristics make information sharing, incident/vulnerability reporting, incident handling, and oversight difficult. These difficulties have cybersecurity implications that may grow as decentralised fintech like blockchain become more of a presence in the financial system.

Lastly, this paper considers (re)insurance and rapid response mechanisms for strengthening local and systemic financial resilience. At present, much cyber insurance does not cover cyber war or terrorism.[14] These exclusions contribute to both financial and cybersecurity risks. Therefore,

- This paper considers how to *handle the financial repercussions* of large cyber incidents (incl. cyber warfare and cyber terrorism) at the EU-level.

Summary of policy suggestions for streamlining incident and vulnerability reporting:

1) A cyber (reporting) hub reserved for financial institutions of magnitude that is a component of the Joint Cyber Unit, and works closely with both EU-CyCLONe and the Commission's proposed European vulnerability repository to form a wider information

<https://www.enisa.europa.eu/news/enisa-news/enisa-launches-public-consultation-for-first-candidate-cybersecurity-certification-scheme> accessed 10 September 2020; 'Challenges to Effective EU Cybersecurity Policy' (*European Court of Auditors* 2019) 36; General Secretariat of the Council, 'Council Conclusions on Regulatory Sandboxes and Experimentation Clauses as Tools for an Innovation-Friendly, Future-Proof and Resilient Regulatory Framework that Masters Disruptive Challenges in the Digital Age' [2020] 13026/20.

[13] Claudia Ng, 'Regulating Fintech: Addressing Challenges in Cybersecurity and Data Privacy', (*Harvard Kennedy School,* 22 February 2018) <www.innovations.harvard.edu/blog/regulating-fintech-addressing-challenges-cybersecurity-and-data-privacy> accessed 6 June 2020; 'Decentralised Financial Technologies: Report on Financial Stability, Regulatory and Governance Implications' (*Financial Stability Board,* 2019) 1-3.

[14] Patrick Bracher, 'Cyber Insurance and the War Exclusion | Financial Institutions Legal Snapshot' (*Norton Rose Fulbright: Financial Institutions Legal Snapshot*, 16 July 2019) <www.financialinstitutionslegalsnapshot.com/2019/07/cyber-insurance-and-the-war-exclusion/> accessed 6 March 2020; Felton Johnston, 'Cyberwar/Cyberterrorism—A Challenge For Insurers and Cross-Border Investors' (*Robert Wray PLLC*, 28 May 2019) <www.robertwraypllc.com/cyberwar-cyberterrorism-a-challenge-for-insurers-and-cross-border-investors/> accessed 25 September 2020; Simon Shooter, 'Cyber Insurance: Debunking the Myths' (*Bird & Bird LLP* and *Lexicology*, 28 June 2019) <www.lexology.com/library/detail.aspx?g=26cddd55-b7ab-495d-b832-afc4a37fcac1> accessed 24 September 2020.

sharing and advisory cyber hub, could mitigate systemic risk while being more politically feasible than proposals for an EU-wide pan-sectoral hub.

2) Report submission mechanisms could be further harmonised into a dynamic online form that automatically adjusts and includes all relevant fields per selected sector and sub-sector.

3) Multi-stage incident reporting for which a template includes the full range of information prompts for a given (sub)sector at every stage could facilitate the capture of as much pertinent information as early as possible. The reporter need only answer the prompts that they can at any given stage.

4) Making a controller's collection of compensation from processors as per GDPR more explicitly dependent on the quality of oversight could reinforce third-party+ oversight.

5) The European Union Agency for Cybersecurity (ENISA) and member states could strengthen vulnerability reporting and reduce systemic risk by (1) encouraging the development of Coordinated Vulnerability Disclosure (CVD) manifestos at the (sub)sectoral level(s), (2) further consolidating vulnerability reporting at the EU-level, and (3) normalising the rapid, anonymous sharing of reports with relevant institutions.

Summary of policy suggestions for mitigating tensions between law and emerging technologies:

6) Annual ENISA reviews of certification frameworks for emerging fintech, that facilitate the reappraisal of relevant regulations, could strengthen financial cybersecurity by improving the relationship between law and fintech.

7) Aspects of the federal regulatory sandbox bill that is pending in the United States House of Representatives could serve as inspiration for an EU-level sandboxing framework.

8) A softly-centralised governance and oversight entity for financial blockchain networks in the EU could help to build consensus, harmonise standards, and improve the reporting and handling of incidents/vulnerabilities for financial blockchains.

Summary of policy suggestions for strengthening local and systemic financial resilience:

9) A European commercial cyber risk pool that covers acts of cyber warfare/terrorism could build further resilience against cyber-induced financial risk. Such a pool would mitigate the widespread exclusion of cyber warfare/terrorism from insurance plans.

10) A rapid response fund for infrastructural patching and incident handling costs that is associated with such a pool could further mitigate systemic risk.

11) A publicly-backed rapid response fund for infrastructural patching and incident handling costs could complement the private-sector response fund once the latter is exhausted.

12) An additional layer of public backing for bank resolutions caused by acts of cyber warfare/terrorism would further mitigate cyber-induced systemic risk. Public funding is warranted by the national security and geopolitical implications of cyber war/terrorism.

I. INTRODUCTION

Policy makers and researchers are paying increasing attention to financial cybersecurity in the Eurozone. The cross-border nature of cyberattacks and their effect on integrated financial networks are particular causes of concern. Although significant strides in policy are being made, the Eurozone's financial cybersecurity still faces a number of challenges. Notable among these challenges are an approach to cybersecurity that could be more harmonised than it is currently, the possibility of cyber-induced financial risk, and the technological and regulatory challenges posed by emerging technologies. This paper considers ways in which to reinforce financial cybersecurity in the Eurozone with respect to these three themes and their areas of overlap. This paper's approach to reinforcement includes the further harmonisation and streamlining of relevant cybersecurity frameworks. Importantly, another aspect of the harmonisation and streamlining approach outlined here is the mitigation of cyber-induced financial risk once an incident has occurred. Consequently, this paper not only deals with frameworks concerning the cyber aspect but also with those focused on the post-incident, financial aspect.

The Eurozone's experience of the 2008–2012 Global Financial Crisis, as well as the increase in cross-border attacks and the Eurozone's high financial integration, have brought attention to systemic risk and the degree to which cybersecurity regulation, administration, and infrastructure should be harmonised in the Eurozone.[15] Although the extent to which financial cybersecurity frameworks in the Eurozone should be independent or united is not a new issue, it has become a more pressing one in the wake of Europe's twenty-first century experience of systemic instability. Attempts to pre-empt and mitigate systemic instability have resulted in steps toward a banking union, which so far includes the Single Supervisory Mechanism (SSM) and the Single Resolution Mechanism (SRM).[16] A Deposit Insurance Scheme is to be added in future. Greater banking harmonisation heightens the issue of greater cybersecurity harmonisation.

The growing severity and complexity of cyber threats also increases the relevance of framework harmonisation and systemic risk for cybersecurity. Following uncertainty in the policy literature

[15] European Systemic Risk Board, *Systemic Cyber Risk* (2020) 52-53; Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance: Getting the policy mix right!–Report of a CEPS-ECRI Task Force* (Centre for European Policy Studies and European Credit Research Institute, 2018) 36-38; Maria Demertzis and Guntram Wolff, 'Hybrid and Cybersecurity Threats and the European Union's Financial System' (*Bruegel*, 2019) 6-11.
[16] Marcel Magnus, 'Banking Union' (*Factsheets on the European Union: European Parliament,* December 2019) <www.europarl.europa.eu/factsheets/en/sheet/88/banking-union> accessed 20 July 2020.

about the likelihood of cyber-induced systemic instability, the European Systemic Risk Board (ESRB) emphasised the possibility in a February 2020 report and expressed its commitment to developing the necessary safeguards.[17] While past attacks have not been able to generate a contagion of low confidence in the financial system, they have demonstrated the increasing ability for strikes to occur effectively and rapidly across integrated networks.[18] The ESRB's study recognises that a liquidity crisis and a corresponding loss of market confidence could occur if a cyber incident of scale tampers with monetary values held in the financial system.[19] Since market confidence can vault a cyber incident into a systemic risk, the ESRB report emphasises the need for efficient information sharing mechanisms as well as clear jurisdictions for dealing with the many facets of such a crisis.[20]

It is in light of greater financial integration and growing cyber capabilities that two central themes of this paper are how to further (1) mitigate **cyber-induced financial risk** and (2) improve **cybersecurity harmonisation** in the Eurozone. Within these two themes, *information sharing* and *incident/vulnerability reporting* are important areas with which policy researchers and makers are increasingly engaging. Good incident/vulnerability reporting and disclosure policies mitigate cyber-induced financial risk by facilitating coordinated incident pre-emption and handling. Reinforcing *oversight* as much as possible is also important. Doing so improves the quality of incident reports and the process of information sharing.[21] It also mitigates third-party+ risk.[22] In a financial system as integrated as the Eurozone, a coherent approach to information sharing, incident and vulnerability reporting, and oversight is essential for mitigating localised and systemic financial risk. So too is a coherent approach to *insurance* as well as *solidarity for cyber-induced financial risk*.

This paper's third policy theme, which overlaps with the other two just mentioned, is (3) the relationship of cybersecurity, regulation, and **emerging financial technologies** (fintech). Efforts to improve information sharing, incident/vulnerability reporting, and oversight need to take into

[17] Christine Lagarde, 'Remarks on the Occasion of Receiving the Grand Prix de l'Économie 2019 from Les Echos', (*ECB*, 2020) <https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200205_1~cc8a8787f6.en.html> accessed 28 February 2020; European Systemic Risk Board, *Systemic cyber risk* (2020); Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance: Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (*CEPS-ECRI*, 2018), 36-38.
[18] ibid., 2.
[19] ibid., 3.
[20] ibid.
[21] 'The Privileged Access Threat Report 2019' (*BeyondTrust*, 2019) <www.beyondtrust.com/resources/whitepapers/privileged-access-threat-report> accessed 5 May 2020.
[22] ibid.

account the unprecedented characteristics of important emerging fintech into account It is important to *facilitate the compliance of emerging financial technologies*—which often have unconventional features—by encouraging *regulations* that enable incident reporting and oversight. . Compatibility problems between emerging fintech and existing regulation can undermine the secure integration of emerging fintech, especially across multiple jurisdictions that have different regulatory standards. Such disjunction and regulatory ambiguity can create legal and technical vulnerabilities in the financial system which cyber attackers can exploit. It is conceivable that such issues like these could facilitate incidents that result in cyber-induced systemic instability.

Outline of the Policy Areas and Suggestions

This paper:

(1) *...engages with the idea of an EU-level cyber (reporting) hub that reinforces planned and existing incident analysis and information sharing mechanisms.* An EU-level hub has become a growing topic in the policy literature. This paper puts forward suggestions on this front that are focused on balancing a drive towards greater harmonisation with a consideration of current political and practical feasibility at this stage. It outlines a cyber (reporting) hub composed of those cross-border financial institutions of magnitude that pose the highest systemic risk. The cyber (reporting) hub would be a component of the Joint Cyber Unit and would complement and work closely with the Commission's proposed European Cyber Crises Liaison Organisation Network (EU-CyCLONe). It would also work closely with the Commission's proposed European vulnerability repository and could potentially play a role in vulnerability reporting and information sharing. The reporting hub, EU-CyCLONe, and the repository could all be viewed as components of an integrated reporting, information sharing, analysis, and advisory hub.

(2) *...suggests reinforcing third-party+ oversight* through revising the existing GDPR provision that allows controllers to claim compensation from compromised third-party+ vendors that fall within the definition of processors and were insufficiently prepared. Such compensation could be made explicitly conditional upon the controller having had strong oversight.

(3) *...assesses existing EU frameworks for detecting, reporting, and disclosing software vulnerabilities in financial technologies.* An attempt is made to balance the freedom of the private sector to establish CVD agreements that are most suitable for a given company with a move towards greater harmonisation. Building on precedents set by sectoral manifestos in the Netherlands, this paper suggests that ENISA and national governments should encourage the

development of manifestos for CVD at various levels of a given sector. Such manifestos establish shared standards while allowing customisability for subsets of a sector. This paper also suggests further centralising vulnerability reporting at the EU-level and normalising the *rapid*, anonymised sharing of vulnerability information with relevant entities.

(4) *...considers ways in which disjunctions between regulation and emerging fintech can be narrowed.* This paper covers strategies for improving the relationship between regulation and emerging technologies in a manner that contributes to cybersecurity harmonisation across member states. Such strategies include more frequent reappraisal of this relationship. This paper also encourages the spread of regulatory sandboxing for emerging fintech and outlines a framework for an EU-level regulatory sandbox that is modelled on a pending proposal for a US version.

(5) *This discussion is followed by a closer look at a particular type of the emerging technology. Namely, decentralised fintech like blockchain.* This choice of case study is motivated by the financial sector's increasing experimentation with decentralised fintech and the challenges that such technology pose for information sharing, incident/vulnerability reporting, and oversight. This paper puts forward suggestions for a softly-centralised governance and oversight entity/consortium for financial blockchains in the EU. This entity would be composed of private-sector participants in cooperation with relevant public-sector stakeholders and would help to build consensus, harmonise standards, and improve the reporting and handling of incidents and vulnerabilities with respect to blockchain.

(6) The paper then turns from policy areas that can lessen financial risk before and during cyber incidents to measures that can mitigate the proliferation of cyber-induced financial instability once an incident has already occurred. The paper looks at how to handle a gap in the insurance market caused when providers do not cover losses that fall under cyber warfare or cyber terrorism. *This paper suggests a European commercial (private-sector) cyber risk pool that explicitly covers cyber warfare and cyber terrorism and can rapidly respond to the afflicted financial system's infrastructural and operational needs.*

(7) The paper then moves on to consider the role of public funding in mitigating the effects of cyber incidents on the financial system. It considers the need for a publicly backed fund that complements the commercial cyber risk pool's rapid response fund once the latter is exhausted. In light of the fact that cyber warfare and cyber terrorism are national security issues with

geopolitical implications, the paper also considers whether an additional layer of direct public backing for bank resolution is warranted.

Towards Greater Harmonisation and Coherence

Many of the suggestions put forward in this paper give momentum to greater harmonisation and, in some cases, to greater centralisation. Conscious not to overstate the normative value of centralised frameworks[23], however, consideration is given to sectoral and regional needs. Many of the suggestions are also made in consideration of the benefits of more decentralised and partially harmonised systems that are currently more politically attainable at this point in time and which can potentially serve as building blocks for more cohesive frameworks in the future.

It is important to note the value in allowing local adaptation. Although greater cohesion and harmonisation are sometimes best achieved through greater centralisation, they are not always best achieved in that manner. The paper thus offers more and less centralised policy options that can complement one another and raise the average degree of coherence towards financial cybersecurity across the Eurozone. This paper thus promotes greater harmonisation and coherence without equating these characteristics to homogenisation.

[23] Helena Carrapico and Andre Barrinha, 'The EU as a Coherent (Cyber)Security Actor' [2017], JCMS 55(6) 1267.

II. BACKGROUND ON EXISTING FRAMEWORKS

There is room to further reinforce the Eurozone's financial cybersecurity, but the EU is still on its way to achieving its goal of being a leader in cyber competence.[24] Significant strides have been made to develop a concerted approach. Recent progress includes the 24 September 2020 proposals for regulation on 'digital operational resilience for the financial sector', for 'a pilot regime for market infrastructures based on distributed ledger technology', and for markets in crypto-assets, as well as the 16 November 2020 Council Conclusions on 'Regulatory sandboxes and experimentation clauses'.[25] On 16 December 2020, the European Commission released a new EU Cybersecurity Strategy and proposals for a revised NIS Directive that look to foster greater cooperation between member states.[26]

This section outlines current pertinent EU regulations, proposals, and entities and the potential pillars for cybersecurity in the Eurozone. There are many components to European cyber policy and this is why only an overview of some of the core elements that are relevant to the policy areas addressed can be attempted here. Therefore, an overview of some of the last decade's seminal developments will be outlined but some frameworks will be discussed in greater detail later in the paper in relation to their relevant sections. Later sections may also touch on additional frameworks where appropriate. A comprehensive interactive 'Cybersecurity Institutional Map' can be accessed on ENISA's website.[27]

[24] Jody Westby, 'Why The EU Is About To Seize The Global Lead On Cybersecurity' (*Forbes Magazine,* 31 October 2019) <https://www.forbes.com/sites/jodywestby/2019/10/31/why-the-eu-is-about-to-seize-the-global-lead-on-cybersecurity/#4b6b78d72938> accessed 20 September 2020; Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN/2013/01 final Preamble 1(1), 2(1), 2(3), 2(4).

[25] Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, 2020/0266 (COD); Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology COM(2020) 594 final; Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and amending Directive (EU) 2019/1937 COM(2020) 593 final; General Secretariat of the Council, 'Council Conclusions on Regulatory Sandboxes and Experimentation Clauses as Tools for an Innovation-Friendly, Future-Proof and Resilient Regulatory Framework that Masters Disruptive Challenges in the Digital Age' [2020] 13026/20..

[26] 'The EU's Cybersecurity Strategy for the Digital Decade' (*European Commission*, 16 December 2020) <https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade> accessed 18 December 2020; Joint Communication to the European Parliament and the Council.
The EU's Cybersecurity Strategy for the Digital Decade [2020] JOIN 18 final; NIS Directive II.

[27] 'Cybersecurity Institutional Map' (*ENISA*) <www.enisa.europa.eu/about-enisa/cybersecurity-institutional-map/results> accessed 20 December.

i. ENISA (2004, 2019)

The European Union Agency for Network and Information Security (ENISA) was founded in 2004 and reinforced by the Cybersecurity Act adopted in April 2019.[28] ENISA is a member of the NIS Cooperation Group. It acts as a secretariat within the CSIRTs Network in a supportive role.[29] It works on 'operational cooperation within the CSIRTs network' and helps member states with maturing their National Cyber Security Strategies.[30] ENISA improves capacity building by advising on cybersecurity issues and aiding information sharing.[31] It also runs 'cybersecurity exercises at Union level'[32] and attends international exercises.[33]

This agency is integral to cyber policy and law formulation.[34] It is involved in these respects both at the EU and sectoral levels and advises the Commission on agreements with non-EU countries.[35] At the implementation stage, ENISA is in charge of facilitating consistency by serving as a common point of reference.[36] In addition, it plays a core role in assessing, developing, and advising on a common cyber certification framework.[37] It re-evaluates this framework within every five years.[38] ENISA's certification competencies are part of its goal to improve the harmonisation of the single market[39] and, through its neutrality and transparency, aims to foster appropriate levels of trust towards vetted digital frameworks in the EU.[40]

ENISA also conducts research and publishes reports on cybersecurity issues.[41] This includes reports on incidents, cybersecurity trends, best practices, the cybersecurity market, and emerging technologies.[42] It takes a forward-looking approach in its reports and assists the European Commission on innovation initiatives.[43] Its reports address both the public and private sectors.

---

[28] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency [2004] OJ L 77.
[29] Cybersecurity Act Art. 7.
[30] ibid.
[31] Cybersecurity Act Art. 6.
[32] Cybersecurity Act Art. 6, 7.
[33] Cybersecurity Act Art. 12.
[34] 'European Union Agency for Cybersecurity (ENISA)', (*Official Website of the European Union,* 6 January 2020) <https://europa.eu/european-union/about-eu/agencies/enisa_en> accessed 24 January 2020.
[35] Cybersecurity Act Art. 5, 12.
[36] ibid. 5, 12.
[37] Cybersecurity Act Art. 49.
[38] ibid.
[39] Cybersecurity Act Art. 3.
[40] 'About ENISA – The European Union Agency for Cybersecurity: Towards a Trusted and Cyber Secure Europe' (*ENISA,* 2020) <https://www.enisa.europa.eu/about-enisa> accessed 2 August 2020.
[41] 'European Union Agency for Cybersecurity (ENISA)', (*Official Website of the European Union,* 6 January 2020) <https://europa.eu/european-union/about-eu/agencies/enisa_en> accessed 24 January 2020.
[42] Cybersecurity Act Art. 7, 8, 9.
[43] Cybersecurity Act Art. 9, 11.

ENISA also seeks to facilitate cooperation between and among these sectors and confers with them when developing guidelines.[44] ENISA is proactive in educating the public and private sectors, as well as the wider public.[45] In addition, it liaises with non-EU countries on best practices[46] and is also involved in the development of cyber education across the Union and the improvement of cyber hygiene.[47] ENISA identifies and informs EU and member state authorities about cybersecurity areas that require more research and resources.[48]

See also:

- Sub-section III.I.iv. for existing role in the CSIRTs Network.
- Sub-section IV.IV.ii. for suggested role in regulatory review and regulatory sandboxing.

ii. The European Cybersecurity Strategy (2013, 2020)

The 2013 European Cybersecurity Strategy articulates the EU's aim of becoming a global leader in cybersecurity. It put forward five goals that still continue to guide its approach to cybersecurity. The Joint Communication articulates these goals as follows:[49]

1) 'Achieving cyber resilience.'
2) 'Drastically reducing cybercrime.'
3) 'Developing cyber-defence policy and capabilities related to the Common Security and Defence Policy (CSDP).'
4) 'Develop the industrial and technological resources for cybersecurity.'
5) 'Establish a coherent international cyberspace policy for the European Union and promote core EU values.'

The Cybersecurity Strategy articulates the need to strike a balance between harmonisation at the EU level and initiative at the member state level.[50] To strike this balance, it sets out the following relationships between EU and national actors: (1) 'coordination between NIS competent

[44] 'About ENISA – The European Union Agency for Cybersecurity: Towards a Trusted and Cyber Secure Europe' (*ENISA,* 2020) <https://www.enisa.europa.eu/about-enisa> accessed 2 August 2020.
[45] Cybersecurity Act Art. 10.
[46] Cybersecurity Act Art. 12.
[47] 'Cybersecurity Education' (*ENISA,* 2020) <https://www.enisa.europa.eu/topics/cybersecurity-education> accessed 1 August 2020.
[48] Cybersecurity Act Art. 11.
[49] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN/2013/01 final 2.
[50] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN/2013/01 final 3.

authorities/CERTs, law enforcement and defence' and (2) 'EU support in case of a major cyber incident or attack'.[51]

Plans for the updated European Cybersecurity Strategy were communicated on 16 December 2020. The new strategy includes plans for a Joint Cyber Unit and a European Cyber Shield, which are outlined in this section in greater detail, in II.xix. and II.xx. respectively. The communication touches on proposed revisions to the NIS Directive: the 'development of secure technologies across the whole supply chain'; 'the next generation of broadband mobile networks', '[a]n Internet of Secure Things'; '[g]reater global Internet security' including 'a public European DNS resolver service'; a 'Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres'; a 'Cyber-skilled EU workforce'; the reinforcement of 'cyber defence capabilities'; 'EU leadership on standards, norms and frameworks in cyberspace'; 'cooperation with partners and the multi-stakeholder community'; 'strengthening global capacities to increase global resilience'; and the bolstering of 'cybersecurity in the EU institutions, bodies and agencies'.[52]

iii. The European Cybercrime Centre (2013)

The European Cybercrime Centre '[pools] European cybercrime expertise to support Member States' cybercrime investigations and provid[es] a collective voice of European cybercrime investigators across law enforcement and the judiciary.'[53]

iv. Cyber Defence Policy Framework (2014, 2018)

The initial 2014 framework is a follow-up to the 2013 EU Cybersecurity Strategy focused on developing the issue of cyber defence highlighted in that Strategy.[54] It approaches cyberspace as its own area of warfare and outlines six priorities. These priorities build on the Common Security and Defence Policy (CSDP) and complement the Cybersecurity Strategy:

1) 'Supporting the development of Member States cyber defence capabilities...'
2) 'Enhancing the protection of CSDP communication networks used by EU entities.'

[51] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN/2013/01 final 3.
[52] Communication from the Commission on the EU Security Union Strategy [2020] COM(2020) 605 final IV(1) 5-24.
[53] 'Cybercrime', (*European Commission*) <https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en> accessed 10 March 2020; Treaty No. 185 The Convention on Cybercrime of the Council of Europe [2001] ETS 185.
[54] EU Cyber Defence Policy Framework [2014] DG C 2B 15585/14 Annex.

3) 'Promotion of civil-military cooperation and synergies with wider EU cyber policies, relevant EU institutions and agencies as well as with the private sector.'
4) 'Research and technology in cooperation with the private sector and academia.'
5) 'Improv[ing] training, education and exercises opportunities.'
6) 'Enhancing cooperation with relevant international partners' such as NATO.

The 2018 framework updates the implementation goals and details of these priorities.[55]

v. The European Agenda on Security (2015)

The cyber component of the European Agenda on Security articulates a commitment to cybersecurity and assertive action against cybercrime.[56] Its proposals include:

- 'Ensuring full implementation of existing EU legislation....'
- Greater cross-border cooperation between 'competent judicial authorities'.
- Public-private partnerships that facilitate investigations while honoring data protection.
- Europol's European Cybercrime Centre as an 'information hub for law enforcement'.

vi. The Digital Single Market Strategy (2015)

In addition to outlining the aims of the GDPR and the NIS Directive (see below), the cybersecurity aspect of the Digital Single Market Strategy asserts the need for a more concerted and harmonised follow up to the 2013 European Cybersecurity Strategy with respect to improving 'industrial and technological resources for cybersecurity'.[57] Therefore, the Digital Single Market Strategy announced the Public-Private Partnership on Cybersecurity, as well as a re-evaluation of the e-Privacy Directive (2002) after the launch of the GDPR. The e-Privacy Directive is a set of data protection rules tailored to electronic communication services.[58]

Private-Public Partnership on Cybersecurity (2016)

The cPPP is a partnership between the European Commission and the private-sector European Cyber Security Organization to develop 'a competitive European cybersecurity ecosystem, to

[55] EU Cyber Defence Policy Framework (2018 update) [2018] RELEX.2.B/14413/18.
[56] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions the European Agenda on Security COM/2015/0185 final 3(3).
[57] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Single Market Strategy for Europe [2015] SWD/2015/100 final 3(4)
[58] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201.

support the protection of the European Digital Single Market with trusted cybersecurity solutions, and to contribute to the advancement of the European digital autonomy.'[59] The cPPP pools public-private resources to spur the cybersecurity market and innovation.

vii. The Global Strategy for the EU's Foreign and Security Policy (2016)

The cyber component of the Global Strategy reaffirms the EU's aim to take a leading role in cybersecurity at the global level. It articulates the intention to make cyber considerations pervasive within the union. It also outlines a commitment and framework for cyber diplomacy with other international actors.[60]

viii. Cyber Infrastructure Fund (2016)

A cyber fund is a pool of resources dedicated to improving and enhancing cybersecurity. The EU invests in infrastructure via the Connecting Europe Facility (CEF) programme.[61] In 2018, the EU's CEF Telecom call for cybersecurity proposals extended €11.4 million to thirty-three projects.[62] These projects intend to improve the EU's efficiency in dealing with cyber threats and incidents. Some of the beneficiaries of the fund include Computer Security Incident Response Teams (CSIRTs), Operators of Essential Services, and National Competent Authorities. The fund will enable them to develop or acquire the relevant tools and skills to comply with the NIS Directive (Directive 2016/1148).[63]

See also:

- Sub-sections III.VII.iii. and IV.VII.i. for *rapid* response infrastructural patching.

ix. The General Data Protection Regulation (2016)

The GDPR (adopted in 2016) applies to processing personal data pertaining to any EU resident, employee, or 'natural person' which is not carried out by a 'natural person in the course of a

[59] 'About ECSO' (*European Cyber Security Organisation*) <https://ecs-org.eu/about> accessed 22 September 2020 (qu.); Commission Decision of 5.7.2016 on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation C/2016/4400 final.
[60] 'Shared Vision, Common Action: A Stronger Europe—A Global Strategy for the European Union's Foreign and Security Policy'(*European Union External Action Service*, 2016); 'EU Global Strategy' (European Union External Action) <https://eeas.europa.eu/topics/eu-global-strategy_en?page=1> accessed 21 September 2020.
[61] 'Connecting Europe Facility' (*European Commission*) <https://ec.europa.eu/inea/en/connecting-europe-facility> accessed 20 December 2020.
[62] DG Connect, '33 New EU Funded Projects to Assist EU Member States in Building Up their Cybersecurity Capabilities' (*European Commission,* 30 April 2019) <https://ec.europa.eu/digital-single-market/en/news/33-new-eu-funded-projects-assist-eu-member-states-building-their-cybersecurity-capabilities> accessed 1 March 2020.
[63] DG Connect, '33 New EU Funded Projects to Assist EU Member States in Building Up their Cybersecurity Capabilities' (*European Commission,* 30 April 2019) <https://ec.europa.eu/digital-single-market/en/news/33-new-eu-funded-projects-assist-eu-member-states-building-their-cybersecurity-capabilities> accessed 1 March 2020.

purely personal or household activity' nor falls under a limited range of exclusions largely related to necessary processing carried out by state actors.[64]

The GDPR defines the concept of a *data controller* as 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.'[65]

A *data processor* is 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.[66] Processors ensure the security of any personal data using 'appropriate technical and organisational measures'.[67]

To help clarify what is considered 'appropriate', a number of national Data Protection Authorities (DPAs) and the European Union Agency for Cybersecurity (ENISA) have issued guidance on how this should be applied.[68] Particular focus has been given to the impact a breach would have on the individual data subject.[69] In order to ensure appropriate security, this guidance also requires that appropriate monitoring is carried out to detect data breaches.[70]

Other responsibilities:

- Controllers are responsible for reporting any breach of personal data within seventy-two hours to the national supervisory authority if it is likely that subjects' 'rights and freedoms' are at risk.[71] They should also compile and maintain information about incidents.
- In addition, controllers are required to 'maintain a record of processing activities under its responsibility' and processors 'shall maintain a record of all categories of processing activities carried out on behalf of a controller'.[72]

[64] GDPR Recital 18.
[65] GDPR Art. 4(7).
[66] GDPR Art. 4(8).
[67] GDPR Art. 5(1)(f).
[68] 'Guidelines for SMEs on the Security of Personal Data Processing' (*European Union Agency for Network and Information Security,* 2016) <https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing> accessed 29 January 2020
[69] ibid.
[70] ibid.
[71] GDPR Rec. 73, 85-88, Art. 33; Anthony Woolich, Felicity Burling, Jeremy Kelly, 'All Change—Are You Compliant with the EU General Data Protection Regulation?: Special Update', (*Holman Fenwick Willan LLP,* 2018) 5.
[72] GDPR Art. 30(1)(2).

- In cases where controller-processor relationships are unclear, multiple organisations must organise themselves under a joint controller clause and determine their respective responsibilities by agreement.[73]
- Failure by controllers and processors to fulfil their respective responsibilities can result in investigations, warnings, reprimands, orders to comply, orders to disclose, orders to rectify, orders to erase, orders to restrict, bans, 'suspension of data flows', decertification, and fines.[74]

See also:

- Sub-section III.II.iii. for third-party+ processors.
- Sub-section III.V.iii. for controller-processor ambiguity on blockchain.

x. NIS Directive (2016, 2020/2021)

The Directive on Security of Network and Information Systems (the NIS Directive, brought into effect in 2016) was created as part of the EU Cybersecurity Strategy. It looks to reinforce the network and information systems security of 'operators of essential services' and 'digital service providers'.[75] Operators of essential services are entities that act in specified sectors and meet criteria that are listed in Article 5(2) of the directive and are identified as essential by the member states.[76] The bodies which fall under this heading are generally those that provide services where an interruption would create a significant problem for consumers (e.g., energy suppliers and transport operators).[77] The member states must ensure that these operators 'take appropriate measures to prevent and minimize the impact' of cyberbreaches in the systems used for the provision of the essential services, 'with a view to ensuring the continuity of those services'.[78] The member states themselves can define what is meant by 'appropriate'.[79]

[73] GDPR Art. 26; Carla Bouca, 'EU GDPR Controller Vs. Processor – The Differences' (*Advisera Expert Solutions Ltd.,* 2020) <https://advisera.com/eugdpracademy/knowledgebase/eu-gdpr-controller-vs-processor-what-are-the-differences/> accessed 27 February 2020; 'What Responsibilities and Liabilities Do Controllers Have When Using a Processor?' (*Information Commissioner's Office*, 2019) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/responsibilities-and-liabilities-for-controllers-using-a-processor/> accessed 27 February 2020.
[74] GDPR Art. 58, Art. 83.
[75] NIS Directive, Legislative Acts, 194/2.
[76] NIS Directive Art. 5(2).
[77] Ibid.
[78] ibid.
[79] ibid.

Digital service providers include any legal persons or entities that provide an 'online marketplace', an 'online search engine', or 'cloud computing services'.[80] The digital service provider must take into account 'the security of the systems and facilities', 'incident handling', 'business continuity management', monitoring/auditing/testing, and 'compliance with international standards' when adopting or identifying security measures.[81] The European Commission has issued further implementation regulations 'as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact'.[82] The NIS Directive stipulates that the approach to the supervision of digital service providers is to be '*ex post*' and 'light-touch'.[83] The directive also notes that '[w]here public administrations in Member States use services offered by digital service providers...they might wish to require from the providers of such services, additional security measures beyond what digital service providers would normally offer in compliance,' which can be done contractually.[84]

CSIRT/CERTs Network

According to the NIS Directive, member states must create at least one Computer Security Incident Response Team (CSIRT), also sometimes called the Computer Emergency Response Team (CERT).[85] The role of these teams is to support cybersecurity preventative methods and to respond to cyber incidents or potential cyber-threats. In addition, each 'Member State shall designate a national single point of contact' from among its CSIRT/CERTs to 'ensure cross-border cooperation', as it is not uncommon to have multiple in-country CSIRT/CERTs.[86] Some of these are sectoral, while others reside in state-owned companies, private companies, or even educational bodies that offer reporting and response services.[87]

---

[80] NIS Directive Annex III.
[81] NIS Directive Art. 16(1).
[82] Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact [2018] OJ L 26 [2004] OJ L 77.
[83] NIS Directive Recital 60.
[84] NIS Directive Recital 54.
[85] NIS Directive Article 9; Otmar Lendl, '"National CERT" vs. "National CSIRTs"', (*Computer Emergency Response Team Austria*, 1 August 2018) <https://cert.at/en/blog/2018/8/blog-20180731155524-2252>. CSIRTs is a generic term. CERTs tend to refer to entities that are license by Carnegie Mellon University, which set the CERT standard. CSIRTs and CERTs are sometimes used interchangeably.
[86] NIS Directive Article 8; 'CSIRTs Network' (*CSIRTs Network*) <https://csirtsnetwork.eu/> accessed 20 July 2020.
[87] NIS Directive Article 8; 'CSIRTs Network' (*CSIRTs Network*) <https://csirtsnetwork.eu/> accessed 20 July 2020.

Operators of essential services must 'notify, without undue delay' a CSIRT about any incident which is 'having a significant impact on the continuity of the essential services they provide'.[88] The significance of an impact depends on 'the number of users affected by the incident, in particular users relying on the service for the provision of their own services', 'the duration of the incident', 'the geographical spread with regard to the area affected by the incident', 'the extent of the disruption of the functioning of the service', and 'the extent of the impact on economic and societal activities'.[89] The notification 'shall include information to enable the competent authority or the CSIRT to determine the significance of any cross-border impact'.[90] There is no requirement to notify if 'the digital service provider [does not have] access to the information needed to assess the impact of an incident'.[91]

The competent authority/CSIRT will then inform other member states 'if the incident has significant impact on the continuity of essential services' in that other member state.[92] The incident can also be disclosed publicly by this authority if it is deemed necessary to do so in the interests of wider security.[93]

NIS Cooperation Group

Building on the CSIRTs Network outlined above, the NIS Directive also established the NIS Cooperation Group.[94] The main purpose of this group is 'to support and to facilitate strategic cooperation and the exchange of information among Member States'.[95] Its competencies include 'providing guidance to competent authorities in relation to the transposition and implementation of this Directive', 'exchanging best practices and information', and 'providing strategic guidance to the CSIRTs network on specific emerging issues'.[96]

Commission Proposal for Revising the NIS Directive (NIS II)

On 16 December 2020, the European Commission released a proposed draft for a revised NIS Directive. The revisions seek to significantly strengthen EU cybersecurity by heightening

[88] NIS Directive Art. 14; NIS Directive Art. 15 (3) & (4); NIS Directive Art. 16(4).
[89] NIS Directive Art. 16 (4).
[90] NIS Directive Art. 16 (3).
[91] NIS Directive Art. 16 (4).
[92] NIS Directive Art. 14 (5).
[93] NIS Directive Art. 14 (6).
[94] NIS Directive Art. 11.
[95] NIS Directive II Art. 12; The European Commission, 'NIS Cooperation Group' (*Official Website of the European Union*, 24 July 2020) <https://ec.europa.eu/digital-single-market/en/nis-cooperation-group> accessed 1 August 2020.
[96] NIS Directive II Art. 12.

cooperation between member states through new and improved frameworks and mechanisms, including for peer-review, incident handling, information sharing, crisis management, and coordinated vulnerability disclosure.[97] The revisions strengthen supervision towards essential entities as well as sanctions for pursuing compliance with the directive.[98] The revisions also expand the range of sectors that the directive covers.[99]

New initiatives and frameworks include:

- Making a CSIRT in each member state the national coordinator for CVD.[100]
- Establishing a 'European vulnerability registry'.[101]
- Requiring 'national cybersecurity crisis management frameworks'.[102]
- Less fragmented incident reporting at the national level through 'a single entry point for all notifications required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC'.[103]
- 'Supply chain risk assessments'.[104]
- The European Cyber Crises Liaison Organisation Network (EU-CyCLONe), which will '(a) [increase] the level of preparedness of the management of large scale incidents and crises; (b) [develop] a shared situational awareness of relevant cybersecurity events; (c) [coordinate] large scale incidents and crisis management and [support] decision-making at political level in relation to such incidents and crisis [and]; (d) [discuss] national cybersecurity incident and response plans referred to in Article 7(2)'.[105] The secretariat would be at ENISA.[106]
- 'A biennial report on the state of cybersecurity in the Union'.[107]
- Peer-reviews.[108]
- 'A registry for essential and important entities'.[109]

[97] NIS Directive II Art. 6, 7, 10, 12-13, 16.
[98] ibid., 13, 27.
[99] ibid., 13.
[100] ibid., Art. 6.
[101] ibid.
[102] ibid., Art. 7.
[103] ibid., 24.
[104] ibid., 21, Art. 5, 18.
[105] ibid., Art. 14.
[106] ibid.
[107] ibid., Art. 15.
[108] ibid., Art. 16.
[109] ibid., Art. 25.

- 'Cybersecurity information-sharing arrangements'.[110]
- Sanctions.[111]

See also:

- Sections III.I. and IV.I. for NIS Cooperation Group, CSIRTs Network, single entry points, cybersecurity information-sharing arrangements, and EU-CyCLONe in relation to the (EU-level) cyber hub idea.
- Section III.II. for supply chain risk assessments in relation to third-party+ oversight.
- Sections III.III. and IV.III. for national CVD coordinators and the European vulnerability repository in relation to the (EU-level) cyber hub idea.

xi. The EU's Joint Framework for Countering Hybrid Threats (2016)

The joint framework sets out to prevent, combat, and improve resilience against increasingly complex combinations of cyber, infrastructural, and political attacks. One form of hybrid attack is a cyberattack that is combined with disinformation campaigns and/or attacks on physical infrastructure.[112] The joint framework's definition accounts for the nebulous nature of hybrid threats:

> ...the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare.[113]

The framework complements member states' responsibility for their own security with a capacity to respond jointly to shared hybrid threats. Its proposals are focused on 'improving awareness, building resilience, preventing, responding to crisis and recovering.'[114] Its suggestions to improve awareness include establishing an EU Hybrid Fusion Cell (operational since 2018) and a Centre

[110] NIS Directive II Art. 26.
[111] ibid., 27, 28, Art. 29, 30, 33.
[112] Maria Demertzis and Guntram Wolff, 'Hybrid and cybersecurity threats and the European Union's financial system' (*Bruegel,* 2019).
[113] Joint Communication to the European Parliament and the Council Joint Framework on countering hybrid threats a European Union response [2016] JOIN(2016) 18 final, Introduction.
[114] ibid.

of Excellence for Countering Hybrid Threats (operational since 2017).[115] In addition, the framework outlined the need for working in close cooperation with NATO on these issues.[116]

The European Centre for Excellence for Countering Hybrid Threats (2017)

The Centre brings together representatives from twenty-eight EU and NATO countries to share knowledge about hybrid threats.[117] In cooperation with the European Commission, they have developed a 'conceptual model for the analysis of hybrid threats' to help member countries prepare for and address this variety.[118]

The Hybrid Fusion Cell (2018)

The Hybrid Fusion Cell is a component of the EU Intelligence and Situation Centre which is a branch of the European External Action Service (the EU's foreign relations arm).[119] It plays a research, information gathering, analytical, information sharing, and advisory role on hybrid attacks.[120] It serves as a coordinating point for national points of contact. The Cell is very active and is expanding its personnel.

See also:

- Sub-section IV.I.ii. for hybrid attacks in relation to a cyber hub.
- Sub-section IV.VII.i. for hybrid attacks in relation to a Cyber Emergency Fund.

xii. Cyber Diplomacy Toolbox (2017, 2020)

The Cyber Diplomacy Toolbox, formally known as the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, outlines what responses are appropriate for any given incident.[121] It addresses the extent to which relevant EU actors need to be sure who is responsible

[115] Joint Communication to the European Parliament and the Council Joint Framework on countering hybrid threats a European Union response [2016] JOIN(2016) 18 final 3(1).
[116] ibid., 6.
[117] 'What is Hybrid CoE?: The European Centre of Excellence for Countering Hybrid Threats' (*Hybrid CoE*) <www.hybridcoe.fi/> accessed 19 September 2020; Joint Staff Working Document Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats [2019] SWD(2019) 200 final 5.
[118] Joint Staff Working Document Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats [2019] SWD(2019) 200 final 4-5; 'What is Hybrid CoE?: The European Centre of Excellence for Countering Hybrid Threats' (*Hybrid CoE*) <www.hybridcoe.fi/> accessed 19 September 2020.
[119] Joint Communication to the European Parliament and the Council Joint Framework on countering hybrid threats a European Union response [2016] JOIN(2016) 18 final 3(1).
[120] Joint Staff Working Document Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats [2019] SWD(2019) 200 final 2.
[121] Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities [2017] DGD 2B/13007/17.

for an incident before utilizing a given tool. The list of tools includes statements, démarches, capacity building, international agreements, strategic communication, joint investigations, formal request for assistance, council conclusions, dialogues, a severing of diplomatic relations, the solidarity clause, sanctions, countermeasures, the mutual defense clause, and military response.[122]

The 16 December 2020 communication on the new European Cybersecurity Strategy indicates plans to reinforce the toolbox.[123] The communication proposes to do this through the development of an 'EU cyber intelligence working group residing within the EU Intelligence and Situation Centre (INTCEN)' of given member states so as 'to advance strategic intelligence cooperation on cyber threats and activities'. It also notes that a 'proposal for the EU to further define its cyber deterrence posture' will be forthcoming. Other forthcoming initiatives include an evaluation of 'additional measures under the cyber diplomacy toolbox', an 'update of the implementing guidelines of the cyber diplomacy toolbox', and efforts to 'further integrate the cyber diplomacy toolbox in EU crisis mechanisms'.

xiii. Threat Intelligence-Based Ethical Red (TIBER) Teaming Framework (2018)

TIBER-EU is a resilience framework for testing the European financial system's ability to withstand cyberattacks.[124] It involves cooperation between member state governments, their financial institutions, and the ECB. ENISA is sometimes also consulted for input.[125] Intelligence-led red teams prepare and conduct incident simulations that are tailored to a given financial institution or infrastructure. The EU-level framework explicitly aims to prevent the emergence of different red team frameworks in member states, which would be inefficient and might result in different qualities of testing. TIBER-EU provides a harmonised and consistent framework for testing and improving resilience against cyber incidents that facilitates a common standard of resilience.[126] Given the cross-border nature of both financial institutions and cyber-attacks, TIBER-EU provides more holistic testing for multinational entities. In addition to developing and running tests at the EU-level, TIBER-EU advises national authorities on how they might

[122] Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities [2017] DGD 2B/13007/17; Erica Moret and Patryk Pawlak, 'The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime' (*European Union Institute for Security Studies* 2017) 3.
[123] Communication from the Commission on the EU Security Union Strategy [2020] COM(2020) 605 final IV(1) 16-17.
[124] 'TIBER-EU Framework: How to Implement the European Framework for Threat Intelligence-Based Ethical Red Teaming' (*European Central Bank*, 2018) 2.
[125] ibid., 36.
[126] ibid., 2.

undertake similar testing on their own initiative.[127] TIBER-EU facilitates information sharing as well as harmonised regulations pertaining to oversight and supervision.[128]

The TIBER-EU Knowledge Centre is a forthcoming hub for coordinating, informing, training, and analysing ethical red teaming operations throughout the EU.[129] It connects the TIBER Cyber Teams from across the member states and interacts with relevant EU, national, and sectoral authorities. In addition, the ECB promotes the idea of a chief TIBER Cyber Team that will be in charge of coordinating and overseeing technical operations.[130] This would include ensuring the quality of resilience tests.

See also:

- Sub-section IV.I.ii. for consulting role in suggested cyber hub.
- Sub-section IV.IV.ii. for consulting role in suggested regulatory sandbox framework.
- Sub-section IV.VI.iii. for consulting role in suggested EU commercial cyber risk pool.

xiv. The Cybersecurity Act (2019)

The Cybersecurity Act (2019) further develops ENISA's competencies and outlines a European Cybersecurity Certification Framework.

Expanded Mandate for ENISA

This Act creates an operational role for ENISA and establishes it as a permanent institution. ENISA's extended role reads as follows:

> It should promote the exchange of best practices between Member States and private stakeholders, offer policy suggestions to the Commission and the Member States, act as a reference point for Union sectoral policy initiatives with regard to cybersecurity matters, and foster operational cooperation, both between Member States and between the Member States and Union institutions, bodies, office and agencies.[131]

More detail on ENISA's updated mandate is available in the preceding sub-section on ENISA.

[127] 'TIBER-EU Framework: How to Implement the European Framework for Threat Intelligence-Based Ethical Red Teaming' (*European Central Bank*, 2018) 2.
[128] ibid.
[129] ibid., 15-16.
[130] ibid., 15.
[131] Cybersecurity Act Preamble 17.

The European Cybersecurity Certification Framework

The EU-wide certification framework assesses and certifies ICT digital 'products, services, and processes' for cyber risk and security.[132] It labels a product, service, or process with basic, substantial, or high level security confidence. This label is based on the security tests the product needs to pass. ENISA advises the European Commission on certification, develops new certifications, and reviews existing certifications.[133]

The framework establishes a network of national certification authorities which are in charge of conformity assessment bodies. The conformity assessment bodies monitor the implementation of and compliance with certifications.[134] Certificates are confirmed by the national authorities. The national authorities, therefore, have both monitoring and certification powers. These powers should not encroach upon each other. In order to ensure the separation of powers within national authorities and harmonisation between member states, the national authorities undergo peer review.[135] In addition, information about compliance and ICT developments must be shared between the authorities.[136]

The Act establishes a European Cyber Certification Group (ECCG) composed of the national certification authorities.[137] This ECCG works with the Commission to achieve similar implementation across member states. It also works with ENISA to develop certification schemes, gives feedback on schemes, and advises the Commission about the need to update any schemes. In addition, it is the body that makes the interactions between the national certification authorities outlined above possible. It also assesses the relationship of EU-level and member state certification schemes in comparison to those in effect at the wider international level. If necessary, it can advise ENISA to liaise at the international level with the aim of improving international certification frameworks.

The certification scheme's development and maintenance processes involve a number of cogs. A rolling work programme makes a list of ICT developments to be considered in a certification context, taking into account certification at the national level, market developments, cyber threats,

[132] Cybersecurity Act Art. 48-49.
[133] ibid.
[134] ibid., Art. 58.
[135] ibid., Art. 59.
[136] ibid., Art. 58.
[137] ibid., Art. 62.

and advice from the ECCG.[138] The rolling work programme is revised on a three-year cycle, though this can also be done ad hoc.

The Act goes on to establish a Stakeholder Cybersecurity Certification Group 'composed of members selected from among recognised experts representing the relevant stakeholders'.[139] ENISA can ask for feedback from this group which also works with the Commission to determine what to include or amend on the rolling work programme. It can also 'advise the Commission on strategic issues regarding the European cybersecurity certification framework'.[140]

Both ENISA and the ECCG can develop and review schemes, but ENISA does so for the most part.[141] On occasion, ENISA may receive a request to develop or review a scheme from the ECCG rather than from the usual avenue of the Commission. In such a case, ENISA has the discretion whether or not to develop or review the scheme. ENISA and a special working group attached to a given scheme develop schemes in consultation with the ECCG and stakeholders.[142] Regular reviews of all certification schemes must be conducted within a five-year cycle. The Commission and the ECCG can also make ad hoc requests for review.

See also:

- Sub-sections III.I.i. & iv. for ENISA's expanded mandate in the CSIRTs Network.
- Sub-section IV.IV.i. for ENISA, the certification framework, and agile regulatory review.

xv. Cybersecurity Competence Network and Centre (2018, 2020)

The European Commission proposed a European Cybersecurity Competence Network and Centre in 2018, which was agreed upon in December 2020.[143] The Centre would facilitate innovation in industry, technology, and research. This proposal aims to develop a 'Europe-wide cybersecurity industrial and research ecosystem'.[144] It seeks to improve and harmonise the

[138] Cybersecurity Act Art. 47.
[139] ibid., Art. 22.
[140] ibid.
[141] ibid., Art. 48, 49.
[142] ibid., Art. 49.
[143] Cybersecurity Technology and Capacity Building Unity, 'Proposal for a European Cybersecurity Competence Network and Centre' (*European Commission,* 19 September 2018) <https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre> accessed 1 August 2020; 'Commission Welcomes Political Agreement on the Cybersecurity Competence Centre and Network' (*European Commission,* 11 December 2020) <https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2384> accessed 20 December 2020.
[144] Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018 [2018] COM/2018/630 8.

operation of the EU's cybersecurity frameworks and is intended to facilitate more concerted cooperation between the private and public sectors. It would also provide a concentrated channel for cyber expertise in the EU, which is too often susceptible to 'brain-drain'.[145] At the same time, it proposes to expand the EU's talent pool and heighten cyber hygiene by investing in quality cybersecurity education throughout the Union.[146] It emphasises taking 'a proactive, longer-term and strategic perspective to cybersecurity industrial policy going beyond research and innovation only'.[147] This long-horizon approach would help mitigate the technological challenges posed by emerging cyber technologies, move the EU to the forefront of emerging cyber developments, and reduce the disjunctions between law and emerging tech.

xvi. Proposal on Digital Operational Resilience for the Financial Sector

The Commission released a proposal for regulation on 'digital operational resilience for the financial sector' on 24 September 2020.[148] Proposals with particular relevance to this paper include Article 13 on the 'responsible disclosure of ICT-related incidents or major vulnerabilities', Article 17 on the '[r]eporting of major ICT-related incidents', Article 18 on the '[h]armonisation of reporting content and templates', Article 19 on the 'centralisation of reporting of major ICT-related incidents', and Chapter V on the 'Managing of ICT Third-Party Risk'. These provisions will be engaged with in the relevant sections of this paper.

See Also:

- Sections III.I. and IV.I. for EU-level cyber hub and incident reporting phases and templates discussion.
- Sections III.II. and IV.II. for third-party+ oversight.
- Sections III.III. and IV.III. for coordinated vulnerability disclosure.

[145] Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018 [2018] COM/2018/630 8; Commission Staff Working Document Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres [2018] SWD/2018/403 final 17.
[146] Proposal for the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres [2018] COM/2018/630 6.
[147] ibid., 8.
[148] Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, 2020/0266 (COD).

xvii. Proposal on a Pilot Regime for Market Infrastructures Based on DLT

The expressed purpose of this proposed regulation is 'the experimentation of DLT market infrastructures' and the 'allowing [of] supervisors and legislators to identify obstacles in the regulation, while regulators and firms themselves gain valuable knowledge about the application of DLT'.[149] The pilot regime would '[lay] down requirements on multilateral trading facilities and securities settlement systems using distributed ledger technology "DLT market infrastructures"'. [150] These requirements relate to '(a) granting and withdrawing...specific permissions', '(b) granting, modifying and withdrawing related exemptions', '(c) mandating, modifying and withdrawing attached conditions, compensatory or corrective measures', '(d) operating such DLT market infrastructures', '(e) supervising such DLT market infrastructures' and, '(f) cooperation between operators of DLT market infrastructures, competent authorities and ESMA'.[151] One can apply for '[s]pecific permission to operate a DLT multilateral trading facility' and '[s]pecific permission to operate a DLT securities settlement system'.[152] Incidents would be reported to competent authorities and the European Securities and Markets Authority (ESMA), and ESMA would serve as a coordinator towards competent authorities on matters relating to distributed-ledger technologies (DLT), particularly supervision.[153] The regulation has a five-year review period to ascertain issues that arise in this nascent area.[154]

See also:

- Section III.V. and Sub-Section IV.V.i. in relation to the 'softly-centralised' blockchain governance and oversight entity.

xviii. Proposal on Markets in Crypto-assets

The 24 September 2020 Markets in Crypto-Assets proposal aims to strengthen and harmonise requirements for 'transparency and disclosure', 'authorisation and supervision', 'operation, organisation and governance', consumer protection, and 'measures to prevent market abuse' with respect to many virtual assets.[155] In doing so, it intends to '[ensure] that the EU financial services regulatory framework is innovation-friendly and does not pose obstacles to the application of

[149] Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology COM(2020) 594 final 4.
[150] ibid., Art. 1.
[151] ibid.
[152] ibid., Art. 7, 8.
[153] ibid., Art. 9.
[154] ibid., Art. 10.
[155] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and amending Directive (EU) 2019/1937 COM(2020) 593 final Title I Art. 1.

new technologies'.[156] The draft proposal complements the proposed regulation on 'a pilot regime for market infrastructures based on distributed ledger technology' with an eye to achieving these goals.[157] The draft proposal notably lays out specific regulations to mitigate the systemic instability risks that may accompany potential 'global stablecoins' in future, 'which seek wider adoption by incorporating features aimed at stabilising their value and by exploiting the network effects stemming from the firms promoting these assets'.[158]

See also:

- Sub-section IV.V.i. in relation to current EU blockchain harmonisation initiatives.

xix. Joint Cyber Unit (2020, Forthcoming 2021)

It is expected that the European Commission will have a full proposal for a Joint Cyber Unit (JCU) ready in February 2021.[159] This unit would be a significant step towards a more harmonised EU cybersecurity approach. It intends to 'provide structured and coordinated operational cooperation'.[160] The Commission's 16 December 2020 communication about the new EU Cybersecurity Strategy outlines the JCU as follows:

> A Joint Cyber Unit would serve as a virtual and physical platform for cooperation for the different cybersecurity communities in the EU, with a focus on operational and technical coordination against major cross border cyber incidents and threats... As outlined in the Commission President's Political Guidelines, the Unit should enable Member States and EU institutions, bodies and agencies to make full use of existing structures, resources and capabilities and promote a 'need-to-share' mind-set.
>
> ...The Joint Cyber Unit would not be an additional, standalone body, nor would it affect the competences and powers of national cybersecurity authorities or EU participants. Rather, the Unit would act as a backstop where the participants can draw on one another's support and expertise, especially in the event that various cyber communities are required to work closely together. At the same time, recent events show the necessity for the EU

[156] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and amending Directive (EU) 2019/1937 COM(2020) 593 final 1.
[157] ibid.,
[158] ibid., 4.
[159] Samuel Stolton, "We are a Prime Target,' Schinas says, as Commission strives to Bolster Cyber Resilience' (*Euractiv,* 16 December 2020) <www.euractiv.com/section/cybersecurity/news/we-are-a-prime-target-schinas-says-as-commission-strives-to-bolster-cyber-resilience/> accessed 16 December 2020; Communication from the Commission on the EU Security Union Strategy [2020] COM(2020) 605 final IV(1).
[160] Communication from the Commission on the EU Security Union Strategy [2020] COM(2020) 605 final IV(1).

> to step up its level of ambition and readiness to face the cyber threats landscape and realities. As part of their contribution to the JCU, the EU actors (Commission and EU agencies and bodies) will therefore be ready to increase significantly their resources and capabilities, so as to level up their preparedness and resilience.
>
> The Joint Cyber Unit would fulfil three main objectives. Firstly, it would ensure preparedness across cybersecurity communities; secondly, through information sharing, it would provide continuous shared situational awareness; thirdly, it would reinforce coordinated response and recovery. To achieve these objectives, the Unit should build on well-defined blocks and goals, such as guaranteeing secure and rapid information sharing, improving cooperation among participants, including interaction between Member States and relevant EU entities, establishing structured partnerships with a trusted industry base and facilitating a coordinated approach to cooperation with external partners. In order to do so, based on a mapping of available capabilities at national and EU level, the Unit could facilitate the development of a cooperation framework.[161]

See also:

- Sub-section IV.I.ii. in relation to the suggested cyber hub.

xx. European Cyber Shield (2020)

In the interests of improving information sharing and incident handling across the EU, the European Commission indicated its intention to develop a European Cyber Shield in its 16 December 2020 communication about the new EU Cybersecurity Strategy.[162] Its outline reads as follows:

> The Commission proposes to build a network of Security Operations Centres across the EU43, and to support the improvement of existing centres and the establishment of new ones. It will also support the training and skill development of staff operating these centres. It could commit, on the basis of a needs analysis conducted with relevant stakeholders and supported by the EU Agency for Cybersecurity (ENISA), over EUR 300 million to support public-private and cross-border cooperation in creating national

[161] Joint Communication to the European Parliament and the Council the EU's Cybersecurity Strategy for the Digital Decade [2020] JOIN 18 final 13-14.
[162] ibid., 5.

and sectoral networks, involving also SMEs, based on appropriate governance, data sharing and security provisions.

Member States are encouraged to co-invest in this project. The centres would then be able to more efficiently share and correlate the signals detected and create high-quality threat intelligence to be shared with information sharing and analysis centres (ISACs) and national authorities, and thus enabling a fuller situational awareness. The goal would be to connect, in phases, as many centres as possible across the EU to create collective knowledge and share best practices. Support will be made available to these centres to improve incident detection, analysis and response speeds through state-of-the-art AI and machine learning capabilities and [be] complemented by supercomputing infrastructure developed in the EU by the European High-Performance Computing Joint Undertaking.

Through sustained collaboration and cooperation, this network will provide timely warnings on cybersecurity incidents to authorities and all interested stakeholders, including the Joint Cyber Unit (see section 2.1). It will serve as a real cybersecurity shield for the EU, providing a solid mesh of watchtowers, able to detect potential threats before they can cause large-scale damage.[163]

See also:

- Sections III.I. and IV.I. in relation to the suggested cyber hub.

xxi. Cybersecurity Budget for 2021-2027

The European Commission's 2021-2027 budget for the Digital Europe Programme looks to be €7.5 billion. Of that amount, €1.7 billion would be distributed across four cybersecurity areas:[164]

- 'Strengthening cybersecurity coordination between Member States tools and data infrastructures.'
- 'Support[ing] the wide deployment of the cybersecurity capacities across the economy.'
- 'Boost[ing] Europe's capabilities in optical communications and cybersecurity through Quantum Communication Infrastructures.'

[163] Joint Communication to the European Parliament and the Council the EU's Cybersecurity Strategy for the Digital Decade [2020] JOIN 18 final 6-7.
[164] 'EU Budget for the Future' (*European Commission*, 2020); 'Digital Europe Programme: A Proposed €7.5 billion of Funding for 2021-2027' (*European Commission*, 4 June 2020) <https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu82-billion-funding-2021-2027> accessed 20 December 2020.

- 'Reinforc[ing] advanced skills and capabilities within Member States and the private sector for a uniformly high level of security of network and information systems.'

Of the remaining amount, €2.2 billion goes to supercomputing, €2.1 billion to artificial intelligence, €580 million to 'advanced digital skills', and €1.1 billion to 'ensuring the wide use of digital technologies across the economy and society'.

See also:

- Sub-section IV.I.ii. in relation to the suggested cyber hub.

III. KEY POLICY AREAS: BACKGROUND AND ISSUES

The need for a coherent cybersecurity framework has become a fixture of the EU policy rhetoric and official agenda. Diverse cybersecurity frameworks can make cooperation difficult by affecting the ability to effectively share information, report incidents, and undertake joint cyber action.[165] In addition, member states are frequently reluctant to share information due to concerns about national/regional security and/or reservations about the extent of political and financial union.[166] Some member states, such as the members of the Central European Cybersecurity Platform, prefer to keep information sharing regional.[167]

Fragmentation is evident across various aspects of cyber incident and vulnerability reporting. At present, only Lithuania, France, and the Netherlands have national policies for how to report software vulnerabilities that security researchers discover in a company's system.[168] Although incident reporting frameworks are more developed and are found across all EU member states, there have been a wide variety of reporting mechanisms, which range from email to online forms.[169] The type and extent of information that the reporter is required or prompted to provide by these different reporting mechanisms varies greatly between and within member states.[170]

In addition, member states have implemented the 2016 Network and Information Systems (NIS) Directive in different ways.[171] According to the NIS Directive, each member state needs to have a 'national point-of-contact' for cybersecurity issues that collects incident reports and coordinates with other national points-of-contact when cross-border cyber incidents occur. While the majority of member states have a single authority for regulating cybersecurity and handling cyber incidents, in some countries, regulatory competencies and the collation of incident reports remain spread across different sector-specific agencies.[172] In such cases, one of the sectoral

[165] Helena Carrapico and Andre Barrinha, 'The EU as a Coherent (Cyber)Security Actor' [2017], JCMS 55(6) 1265.
[166] ibid., 1264.
[167] ibid., 1264-1265.
[168] Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) 13-23; Erik Silfversten, et al. *Economics of Vulnerability Disclosure*, (*European Union Agency for Network and Information Security*, 2018) 39.
[169] 'Reporting a Cyber Security Incident', (*National Cyber Security Centre UK*) <https://report.ncsc.gov.uk/> accessed 20 April 2020; 'Netherlands (NL)', (*Cyberwiser.eu: Cyber Range and Capacity Building in Cybersecurity,* 2018) <www.cyberwiser.eu/netherlands-nl> accessed 20 April 2020; Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) 2, 14-15.
[170] 'EU National Strategies', (*Cyberwiser.edu: Cyber Range and Capacity Building in Cybersecurity*, 2018) <https://www.cyberwiser.eu/cartography> accessed 20 April 2020. See also III.I.iv. of this report.
[171] Helena Carrapico and Andre Barrinha, 'The EU as a Coherent (Cyber)Security Actor' [2017], JCMS 55(6) 1265
[172] Thomas Stubbings, et al., 'Complying with the European NIS Directive: Cybersecurity for Critical Infrastructures' (*KPMG,* 2019) 9.

authorities is elected to be the required national point-of-contact.[173] The set-up in some countries requires some institutions to submit parallel incident reports to different authorities.[174]

While the diversity and sectoral specificity of the NIS Directive's implementation need not, in itself, be problematic for efficient incident reporting and response, the existence of five other EU-level regulations that govern incident reporting and handling for various service providers compounds this situation.[175] The division of labour between sectoral, national, and regional frameworks is, in some cases, still unclear.[176] Even where the relationship is clear, there can be redundancy and inefficiency.[177] A (financial) institution, for example, may need to report incidents to multiple authorities. The number of parallel reports that need to be made depends on the type of service a (financial) institution provides and the character of the incident.[178] Those authorities may have different reporting mechanisms and requirements.[179] In addition, those authorities may also need to subsequently coordinate amongst themselves.[180] The communication and coordination between national, sectoral, and regional actors is sometimes not yet supported by fully-fledged processes and appropriate infrastructures.[181]

The negative effects of persisting degrees of fragmentation are compounded where companies have sub-optimal oversight over their third-party+ vendors.

Significant strides have been made to improve coherence and mitigate these issues. Most recently with the new EU Cybersecurity Strategy, the Commission's proposed revision of the NIS Directive, and the draft regulation on 'digital operational resilience for the financial sector' (see Sub-Sections II.xvi., II.x., II.xix., II.xx.). Even taking these strides into account, however,

[173] Thomas Stubbings, et al., 'Complying with the European NIS Directive: Cybersecurity for Critical Infrastructures' (*KPMG,* 2019) 9.
[174] ibid., 10.
[175] European Banking Federation, *EBF Position on Cyber Incident Reporting* (2019) 1-6.
[176] ibid., 10; Helena Carrapico and Andre Barrinha, 'The EU as a Coherent (Cyber)Security Actor' [2017], JCMS *55*(6) 1264; European Banking Federation, *EBF Position on Cyber Incident Reporting* (2019) 1-6.
[177] Thomas Stubbings, et al., 'Complying with the European NIS Directive: Cybersecurity for Critical Infrastructures' (*KPMG,* 2019) 9-10; Helena Carrapico and Andre Barrinha, 'The EU as a Coherent (Cyber)Security Actor' [2017], JCMS *55*(6) 1264; European Banking Federation, *EBF Position on Cyber Incident Reporting* (2019) 1-6.
[178] European Banking Federation, *EBF Position on Cyber Incident Reporting* (2019) *5*.
[179] Ibid., 1-6; Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) 2, 14-15.
[180] European Banking Federation, *EBF Position on Cyber Incident Reporting* (2019) *5*.
[181] Thomas Stubbings, et al., 'Complying with the European NIS Directive: Cybersecurity for Critical Infrastructures' (*KPMG,* 2019) 9-10; European Banking Federation, *EBF Position on Cyber Incident Reporting* (2019) 1-6; Helena Carrapico and Andre Barrinha, 'The EU as a Coherent (Cyber)Security Actor' [2017], JCMS *55*(6) 1264.

fragmentation is still an issue to consider.[182] This issue is considered in relation to relevant aspects of these recent regulatory initiatives in Sections III.I., III.II., III.III., IV.I., IV.II., and IV.III. Just as the issue of ever-greater union remains contentious in other areas of European policy, it will continue to bedevil European cybersecurity for the foreseeable future.

With respect to forestalling and offsetting cyber-induced financial risk, it is important to develop cyber insurance mechanisms for the financial industry for both the local and systemic levels. In the EU, a cyber insurance market exists but has not yet matured.[183] Issues like information asymmetry and adverse selection that are familiar to the insurance market are exacerbated where the approach to cybersecurity remains fragmented.[184] In addition, many insurers specifically exclude incidents that result from cyber warfare or cyber terrorism, which are on the rise.[185] A reluctance to insure such incidents and the persisting ambiguity surrounding such insurance has the potential to exacerbate drops in market confidence in the event of a significant cyberattack against one or more financial institution(s) that are not expressly insured for acts of cyber war or cyber terrorism.

In the EU, as elsewhere, the difficulties of regulating and integrating some emerging financial technologies affect both the development of the cyber insurance market and the security of the financial system. For example, financial firms have started to explore possibilities for integrating decentralised technologies, like blockchain, into mainstream financial systems.[186] However, by their very nature, it is difficult to identify a hierarchy of responsibility on decentralised technologies. This makes it difficult to comply with hierarchy identification requirements in EU regulations like the GDPR. Such dissonance between regulation and decentralised financial technologies makes it tricky to report and handle incidents on decentralised fintech. Closing the

[182] Joint Communication to the European Parliament and the Council the EU's Cybersecurity Strategy for the Digital Decade [2020] JOIN 18 final 3-4; Helena Carrapico and Andre Barrinha, 'The EU as a Coherent (Cyber)Security Actor' [2017], JCMS 55(6) 1259-1267; European Banking Federation, *EBF Position on Cyber Incident Reporting* (2019) 1-6; NIS Directive II.

[183] European Insurance and Occupational Pensions Authority (EIOPA), *Cyber Risk for Insurers—Challenges and Opportunities* (2019) 4; EIOPA, *Understanding Cyber Insurance—A Structure Dialogue with Insurance Companies* (2018).

[184] Maria Demertzis and Guntram Wolff, 'Hybrid and Cybersecurity Threats and the European Union's Financial System' (*Bruegel*, 2019) 11.

[185] Patrick Bracher, 'Cyber Insurance and The War Exclusion | Financial Institutions Legal Snapshot' (*Norton Rose Fulbright: Financial Institutions Legal Snapshot*, 16 July 2019) <www.financialinstitutionslegalsnapshot.com/2019/07/cyber-insurance-and-the-war-exclusion/> accessed 6 March 2020.

[186] Daniel Malan, 'The Law Can't Keep up with New Tech. Here's How to Close the Gap' (*World Economic Forum*, 21 June 2018), <www.weforum.org/agenda/2018/06/law-too-slow-for-new-tech-how-keep-up/> accessed 10 March 2020.

compliance gap between unconventional fintech and regulations that facilitate reporting, handling, and oversight is important for cybersecurity.

The compatibility between EU regulations and emerging fintech is regularly assessed by the European Union Agency for Cyber Security (ENISA), but the rapid development of the cyber landscape makes it as difficult for standards to keep up with unprecedented technologies as it is for those technologies to comply with regulations as they develop. ENISA re-evaluates European cyber certification schemes within five-year cycles.[187] However, the pace at which fintech develops challenges this time frame.[188] Regulatory sandboxing is another technique for facilitating compatibility between regulations and emerging tech, by which the letter of regulations is relaxed even as consumer protection and cybersecurity requirements are maintained (albeit in ways more suited to the technology under development).[189] However, only a few EU member states have regulatory sandboxes, and the idea of EU-level regulatory sandboxing for a given sector is awaiting further analysis by the European Commission.[190]

The following sections assess these policy areas in greater detail and in relation to one or more of the three overarching issues raised (European security fragmentation, the potential of cyber-induced systemic risk, and the legislative challenges posed by emerging technologies).

[187] Cybersecurity Act Art. 49(8).
[188] Manoj Kashyap et al., 'Blurred lines: How FinTech is Shaping Financial Services—Global FinTech Report', (*PWC*, 2016), 3, 7, 17; Emmet McEvoy, 'Regulation needs to match the pace of fintech innovation' (*Fintech Bulletin,* 18 May 2020) <https://fintech-bulletin.com/regulation-needs-to-match-the-pace-of-fintech-innovation/> accessed 10 September 2020.
[189] 'ECB Announces Support for FintechBank Applicants' (*Lantham & Watkins LLP*, 20 November 2017), <www.latham.london/2017/11/ecb-announces-support-for-fintech-bank-applicants> accessed 1 June 2020.
[190] 'Regulatory Sandboxes', (*Columbia Business School: The Columbia Institute for Tele-Information*, 2016) <https://dfsobservatory.com/content/regulatory-sandboxes> accessed 4 June 2020; ECB Announces Support for FintechBank Applicants' (*Lantham & Watkins LLP*, 20 November 2017), <www.latham.london/2017/11/ecb-announces-support-for-fintech-bank-applicants> accessed 1 June 2020; General Secretariat of the Council, 'Council Conclusions on Regulatory Sandboxes and Experimentation Clauses as Tools for an Innovation-Friendly, Future-Proof and Resilient Regulatory Framework that Masters Disruptive Challenges in the Digital Age' [2020] 13026/20.

III.I. INCIDENT REPORTING AND INFORMATION SHARING

Cyber incident reporting frameworks in the EU have been affected by a significant degree of fragmentation at the EU, member state, and regional levels.[191] The 2018 Centre for European Policy Studies (CEPS) and the European Credit Research Institute (ECRI) Task Force on Cybersecurity in Finance identify three categories of information sharing approaches in the EU: voluntary 'industry-led incident information sharing schemes', EU-level regulatory/supervisory frameworks, and information sharing and analysis centres (ISACs).[192] The industry-led method does not regularly include regulators and supervisors and vice versa.[193] While ISACs engage both sides, cooperation between ISACs has in some cases been suboptimal.[194]

In addition, there are six different EU regulations on cyber incident reporting.[195] These include the NIS Directive (concerning Operators of Essential Services), GDPR (concerning Personal Data Processors and Controllers), eIDAS Regulation (concerning Trust Service Providers), PSD2 (concerning Payment Service Providers), ECB/SSM (concerning 'significant' financial institutions), and ECB Target 2 (concerning participants of the ECB's Real-Time Gross Settlement System).[196] Several of these frameworks stipulate different reporting methods and timelines.[197] Furthermore, the extent of reporting varies, with a considerable role for individual judgment about what to report and when to report it.[198] Several of the regulations listed above also designate different organisations as points-of-contact depending on the type of financial firm affected.[199] The decentralisation and diversity of EU-level agreements has been augmented by diversity and redundancy at the sectoral and national levels.[200] This situation can generate confusion and inefficiency, especially when multiple regulations apply for a single given incident. In light of this situation, Section III.I. discusses the issues of unidirectional reporting processes, restrained and inefficient information sharing, idiosyncrasies between CSIRTs, disparate implementation of EU-level frameworks, and diverse incident reporting templates, which have

[191] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance: Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 12.
[192] ibid., 17-18.
[193] ibid.
[194] Information Sharing and Analysis Centres: Cooperative models' (*ENISA,* 2018) 18-22, 37.
[195] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance: Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 12.
[196] ibid.
[197] ibid.
[198] ibid.
[199] ibid.
[200] European Banking Federation, 'EBF Position Paper on Cyber Incident Reporting' (2019) 1-6; Vangelis Ouzounis, 'Good Practice Guide on Reporting Security Incidents', (*ENISA,* 2009) 18.

had implications for reporting and information sharing practice over the past decade. Section IV.I. considers the extent to which the new EU Cybersecurity Strategy (16 December 2020), the Commission's proposed revision of the NIS Directive (16 December 2020), and 24 September 2020 proposals for new regulations on the financial sector will mitigate these issues. Section IV.I. also puts forward suggestions about how these issues might be further mitigated.

i. Unidirectional Flow

Though the issue of unidirectional incident reporting processes has the potential to be mitigated in conjunction with recently proposed regulations, it is worth noting that many 'authorities in charge' have not previously been in the habit of using incident reports to recommend a course of action to CSIRTs with respect to handling and mitigating a given incident.[201]

Unidirectional flow is expected to become less of an issue for the financial sector through the 24 September 2020 Commission proposal for regulation on 'digital operational resilience for the financial sector'. The proposal states that '[t]o set off a dialogue between financial entities and competent authorities that would help [in] minimising the impact and identifying appropriate remedies, the reporting of major ICT-related incidents should be complemented by supervisory feedback and guidance'.[202]

However, in so far as incidents in other sectors and incidents pertinent to various regulatory frameworks have the possibility of affecting the financial sector (e.g., through hybrid threats), it is important to further mitigate unidirectional flow where it exists. The potential for such mitigation may be found in the Commission's proposed European Cyber Shield, the Joint Cyber Unit (JCU), and EU-CyCLONe (see Sub-Sections II.x., II.xix., and II.xx., and Section IV.I.), but current outlines of these frameworks are not entirely clear about the extent to which authorities in charge might advise CSIRTs. The Cyber Shield will likely improve the advisory situation for Security Operations Centres, but its relationship with CSIRTs is less clear.[203] The extent to which advice from authorities in charge to CSIRTs would factor into the JCU's improved cooperation

[201] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 2, 14 (qu.) 15, 18-19; Joint Communication to the European Parliament and the Council The EU's Cybersecurity Strategy for the Digital Decade [2020] JOIN 18 final 6-7.
[202] Proposal for A Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 COM(2020) 595 final 10.
[203] Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade JOIN(2020) 18 final 6-7.

framework is similarly unclear at this stage.[204] While EU-CyCLONe 'shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements'[205], those arrangements are also yet to be specified.

ii. Restrained and Inefficient Information Sharing

As of the writing of this report, the information sharing framework's tendency to share incident information between relevant CSIRTs has also not been as regular as it might be.[206] Member states are often reluctant to share incident reports that pertain to national security.[207] Some member states—such as the members of the Central European Cybersecurity Platform—prefer to keep information sharing regional.[208] Although there has been an increase in 'information exchange tools and initiatives' across, within, and between various sectors and member states, these initiatives are often regionally- or sectorally-bound.[209] The extent to which these tools and initiatives interact varies greatly, and coordination issues have, in some cases, restrained the framework's effectiveness.[210]

iii. Idiosyncrasies between CSIRTs / Supervisory Authorities

Some CSIRTs have idiosyncratic terms and classifications that make information sharing and coordination across CSIRTs difficult.[211] Four of the six incident-reporting regulations mentioned at the start of this section have reports sent to national authorities rather than to a centralised EU-body.[212] These national organisations control the flow of the information reported to them and how entities report that information.[213] In cases where information is shared, the format in which entities must report information in one jurisdiction can cause misunderstandings in others.[214]

iv. Disparate Implementation and Regulation Multiplicity

While EU-level frameworks already do much to reduce fragmentation, and there are also benefits to local adaptation, it is important to recognise the challenges of diverse

[204] Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade JOIN(2020) 18 final 13-15.
[205] NIS Directive II Art. 14.
[206] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 2, 14, 15, 18-19.
[207] Helena Carrapico and Andre Barrinha, 'The EU as a Coherent (Cyber)Security Actor' [2017], JCMS 55(6) 1264.
[208] ibid., 1264-1265.
[209] Edgars Taurins, 'EU MS Incident Response Development Status Report' (*ENISA*, 2019) 4.
[210] ibid.
[211] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 12-13.
[212] ibid., 12.
[213] ibid., 10-14.
[214] ibid., 12.

implementations.[215] For example, many member states have implemented the NIS Directive in different ways, resulting in diverse incident reporting and information sharing frameworks. The NIS Directive requires each member state to have a national 'point-of-contact' that collects incident reports.[216] While the majority of member states have a single authority for regulating cybersecurity, cybersecurity remains fragmented among sectors in approximately a third of the member states.[217] This is often due to the diverse levels and types of existing cybersecurity infrastructure in a given country. In cases where cybersecurity and incident reporting remains primarily a sectoral affair, the sectoral authorities elect one among their number to be the required national point-of-contact.[218] The national points-of-contact coordinate with one another through the CSIRTs Network when cross-border cyber incidents occur (see Sub-Section II.x.). On the one hand, the CSIRTs Network and ISACs have significantly improved cross-border coordination since 2016 and helped to mitigate the WannaCry incident.[219] Cyber exercises run by ENISA increase the CSIRTs Network's readiness.[220] However, diverse implementations and any corresponding idiosyncrasies can affect the Network's efficiency due to the difficulties of horizontal coordination. In addition, ENISA notes that the multiplicity of ISACs generates significant redundancy and that cooperation between ISACs is limited.[221]

Due to diverse implementations of the incident reporting frameworks, including but not limited to the NIS Directive, there sometimes remains ambiguity in the division of labour between sectoral and national frameworks for reporting and response.[222] In some cases, there also exists ambiguity regarding modes and networks of communication between some relevant authorities at the sectoral, national, and regional levels.[223] Some sectors develop distinct reporting frameworks that are not effectively coordinated with regional or national frameworks.[224] As

[215] 'The NIS Directive' (*Cyberwatching.eu*) <https://cyberwatching.eu/policy-landscape/cybersecurity/nis-directive-and-its-challenges> accessed 21 October 2020.
[216] Helena Carrapico and Andre Barrinha, 'The EU as a Coherent (Cyber)Security Actor' [2017], JCMS 55(6) 1265
[217] Thomas Stubbings et al., 'Complying with the European NIS Directive: Cybersecurity for Critical Infrastructures' (*KPMG,* 2019) 9.
[218] ibid.
[219] Dimitra Markopoulou, Vagelis Papakonstantinou, and Paul de Hert, 'The New EU Cybersecurity Framework: The NIS Directive, ENISA's role and the General Data Protection Regulation' [2019] Computer Law & Security Review 35 7-8.
[220] 'Testing Cooperation of EU CSIRTs Network During Large-Scale Cyber-Attacks' (*ENISA,* 16 May 2019) <https://www.enisa.europa.eu/news/enisa-news/testing-cooperation-of-eu-csirts-network-during-large-scale-cyber-attacks> accessed 21 October 2020. Information Sharing and Analysis Centres' (*ENISA,* 2018) 37.
[221] 'Information Sharing and Analysis Centres: Cooperative Models' (*ENISA,* 2018) 37.
[222] Helena Carrapico and Andre Barrinha, 'The EU as a Coherent (Cyber)Security Actor' [2017] JCMS 55(6) 1264.
[223] European Banking Federation, 'EBF Position Paper on Cyber Incident Reporting' (2019) 1.
[224] ibid., 2; Vangelis Ouzounis, 'Good Practice Guide on Reporting Security Incidents' (*ENISA,* 2009) 18.

discussed above, a given CSIRT or supervisory authority might also have idiosyncratic classifications and reporting mechanisms that affect the ease of horizontal coordination. In addition, sectoral CSIRTs' difficulties in attracting qualified personnel limit their effectiveness.[225] This diversity and fragmentation can cause redundancy and result in the inefficient handling of cross-border cyber-attacks.[226] Diverse implementations of any one of the given six EU-level incident reporting frameworks compound the complications caused by the multiplicity of reporting frameworks. This is especially the case where a given incident falls within two or more of the frameworks and needs to be reported using multiple dimensions.[227]

In light of the above, decentralised and fragmented approaches to incident reporting and information sharing can make it more challenging to understand common threats. Due to different security requirements between countries and within or across regulatory framework(s), a firm may not understand the relevant risks that arise in other jurisdictions.[228] The various formats in which entities report incidents in different jurisdictions can exacerbate these issues.[229] Consequently, it can be difficult for financial firms and supervisory authorities to develop an EU-wide view of relevant cybersecurity risks. Fragmented and diverse approaches to incident reporting are thus a significant cybersecurity issue.

v. Diversity and Thoroughness of Incident Reporting Templates

An aspect of diverse implementation and fragmentation is expressed through incident reporting templates. As of writing of this report, there exist a range of incident and vulnerability reporting templates across the EU. Such diversity poses problems for effective cross-jurisdictional interpretation, for statistical analysis, and for automatic processing of incident reports.[230] There have thus been calls, on multiple fronts including from ENISA and the EBF, to reduce template diversity.[231]

[225] Edgars Taurins, 'EU MS Incident Response Development Status Report' (*ENISA*, 2019) 4.
[226] European Banking Federation, 'EBF Position Paper on Cyber incident reporting' (2019) 1-6.
[227] ibid., 5-6.
[228] ibid., 12-13.
[229] ibid., 12-14.
[230] Vangelis Ouzounis, 'Good Practice Guide on Reporting Security Incidents' (*ENISA,* 2009) 47, 69.
[231] Vangelis Ouzounis, 'Good Practice Guide on Reporting Security Incidents' (*ENISA,* 2009) 47, 69; European Banking Federation, 'EBF Position Paper on Cyber incident reporting' (2019) 7; Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!–Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 12-13.

In response to template diversity that arose from the differential implementation of the eIDAS regulation, ENISA published policy recommendations that help to guide best practice.[232] Concerning the popular two-stage reporting framework, ENISA outlines what content to include in templates at each stage (see Appendix i.).[233] In many versions of the two-stage framework, entities submit the first report as soon as possible, after an incident begins. A subsequent report serves as a follow-up. For the second form, ENISA outlines a template with more technical detail than the first, since this form is generally submitted once the incident is over and the entity has had time to assess the situation in full. ENISA also notes the desirability of multiple reporting stages for incidents of longer duration for which 'the supervisory body might require a regular reporting scheme. E.g., by adding a field to the incident notification for expected next report or by requiring one report at regular intervals during the lifetime of the incident'.[234]

ENISA's recommendations are helpful, but they are guidelines and, thus, not prescriptive. Indeed, ENISA is careful not to assertively promote specific templates that may not be the best fit for individual frameworks.[235] These recommendations, therefore, do not wholly mitigate the diversity of reporting templates, which has remained a significant cybersecurity issue. While the preceding example focuses on eIDAS implementation, because ENISA has explicitly discussed template content in this context, the diversity of templates and reporting channels within the GDPR and NIS frameworks is evident in the CyberWISER Initiative's database.

This database provides a full overview of the GDPR- and NIS-compliant reporting mechanisms, as well as the number of CSIRTs within each member state.[236] Important points of variation include the information required and the extent to which a template offers detailed prompts for information. In many cases, there is no pre-set form, and reporters must simply send an email. As of 2017, European countries that do email reporting as the only or one of the main method(s) include Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France (twelve CSIRTs by email, one by online form), Germany (twelve CSIRTs by email, one by online form), Greece (one CSIRT by email, two by online form), Hungary, Iceland, Ireland, Italy (three CSIRTs by email, one by online form), Latvia, Lithuania (two CSIRTs by email, one by online form), Luxembourg (one CSIRT by email, four by online form, one by either

[232] *Article 19 Incident Reporting: Incident Reporting Framework for eIDAS Article 19* (ENISA, 2016) 30-31.
[233] ibid.
[234] ibid.
[235] ibid.
[236] 'EU National Strategies' (*CyberWISER.eu: Cyber Range and Capacity Building in Cybersecurity*, 2018) <www.cyberwiser.eu/cartography> accessed 20 April 2020.

depending on desired-level of anonymity), Malta, the Netherlands, Norway, Poland (three CSIRTs by email, one by online form), Portugal, Romania (two CSIRTs by email, one by online form), Slovakia, Spain (three CSIRTs by email, three by online form), Sweden, and Switzerland.[237] The extent to which these CSIRTs provide readily accessible and detailed guidance on what to include in an email varies significantly.[238]

In response to this situation, the Commission's proposed draft for the revised NIS Directive (16 December 2020) and proposed regulation on 'digital operational resilience for the financial sector' (24 September 2020) require that more standardised template guidelines be developed. They also require more standardised incident reporting phases. The revised NIS Directive stipulates a two-stage approach, with a brief, first incident report and a more detailed, follow-up report.[239] It asserts that '[t]he initial notification should only include the information strictly necessary to make the competent authorities aware of the incident and allow the entity to seek assistance, if required'.[240] An intermediate report is only to be provided 'upon the request of a competent authority or a CSIRT'.[241] The Commission's proposed regulation on 'digital operational resilience for the financial sector' incorporates more regular intermediate reporting. However, though the proposed regulation notes that '[t]he report shall include all information necessary for the competent authority to determine the significance of the major ICT-related incident and assess possible cross-border impacts', it does not specify the extent to which the templates should have extensive and detailed prompts at each incident reporting stage.[242]

The extent to which reporters are prompted for the sector-specific and technical information that they should provide in an incident report, at any given stage, is another important issue. Sectoral CSIRTs often offer templates that are highly tailored to the sector in question (see Appendix iii. regarding Singapore's financial-specific template). If there is a national CSIRT, sector-specific characteristics and additional technical details of the incident can often be provided in generic write-in fields for additional information if sector-specific templates are not provided. However, even where write-in fields are provided, it is frequently and to a significant extent left to the

[237] 'EU National Strategies' (*CyberWISER.eu: Cyber Range and Capacity Building in Cybersecurity*, 2018) <www.cyberwiser.eu/cartography> accessed 20 April 2020.
[238] ibid.
[239] NIS Directive II 23.
[240] ibid.
[241] ibid., Art. 20.
[242] Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 COM(2020) 595 final Art. 17, 18; NIS Directive II 23.

reporter to determine what sector-specific characteristics are relevant (see Appendix i. for ENISA's eIDAS template guidelines and Appendix ii. for the UK's NCSC reporting template).[243] In the absence of clear prompts or a reporter's thorough consideration of all relevant aspects of the incident, there is a higher risk that pertinent sector-specific considerations and technical details will go unreported at any given stage. Write-in fields can also make it more difficult to interpret a report across jurisdictions depending on the terms and categories the reporter uses.

* * *

As discussed further in Section IV.I., the Commission's proposed revision of the NIS Directive (16 December 2020) seeks to mitigate a number of these issues with new frameworks and initiatives like cybersecurity information-sharing arrangements and EU-CyCLONe. So, too, does the Commission's proposed regulation on 'digital operational resilience for the financial sector'. While these strides will significantly improve incident reporting and information sharing, there is room for further mitigation of these issues. Section IV.I. assesses the potential room for improvement, taking into consideration the revised directive, the digital operational resilience proposal, the Cyber Shield, the JCU, and the policy literature surrounding the idea of an EU-level cyber hub.

[243] 'EU National Strategies' (*CyberWISER.eu: Cyber Range and Capacity Building in Cybersecurity*, 2018) <www.cyberwiser.eu/cartography> accessed 20 April 2020.

III.II. THIRD-PARTY+ OVERSIGHT

With banks increasingly reliant on third-party+ processing (i.e., by third-parties and their sub-contractors), reporting parties and competent authorities need access to reliable information about the extent and nature of a given company's third-party+ network. It is crucial to promulgate and apply regulating measures downstream to third-party+ processors. Third-party+ products and services that do not have adequate cybersecurity or data protection measures frequently introduce vulnerabilities into a system.[244] This issue is often compounded by communication problems between companies and their third-party+ vendors.[245] This section outlines issues that have affected third-party+ oversight, briefly notes the extent to which relevant regulations and proposals mitigate these issues, and highlights an area of GDPR that might be further strengthened to improve controllers' oversight of their processors.

i. Third-Party+ Information Flows and Oversight

There has, in many business areas, been significant distrust between controllers and processors.[246] A 2018 Ponemon Institute report surveyed UK and US companies' relationships with third-party vendors in the context of the GDPR and the California Privacy Act.[247] Only 29% of controllers responded that they would trust vendors to notify them of a data breach and only 43% reported that '[t]hird parties' data safeguards and security policies and procedures are sufficient to prevent a data breach'.[248] As few as 12% 'are confident they would learn that their sensitive data was lost

[244] Michelle Wu, 'Third Party Vendor Breaches Still Major Cybersecurity Issue' (*SecurityScorecard*, 20 July 2016) <https://securityscorecard.com/blog/third-party-vendor-breaches-2016-1> accessed 27 February 2020; 'Insider and Third-Party Access Rank as Top Cyber Threats for Global Organisations' (*BeyondTrust*, 9 May 2017) <www.beyondtrust.com/press/secure-access-report> accessed July 20, 2020; Robin Kurzer, 'Report: Majority of Companies Fear 3rd-Party Vendors Make Them Vulnerable to GDPR Legal Risks' (*MarTech Today*, 31 July 2018) <https://martechtoday.com/report-majority-of-companies-fear-that-3rd-party-vendors-make-them-vulnerable-to-legal-risks-for-gdpr-non-compliance-218922> accessed 1 August 2020.

[245] Ponemon Institute, 'Data Risk in the Third-Party Ecosystem: Third Annual Report' (2018) 2; 'What Responsibilities and Liabilities Do Controllers Have When Using a Processor?' (*Information Commissioner's Office*, 2019) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/responsibilities-and-liabilities-for-controllers-using-a-processor/> accessed 27 February 2020.

[246] Ponemon Institute, 'Data Risk in the Third-Party Ecosystem: Third Annual Report' (2018); 'The Privileged Access Threat Report 2019' (BeyondTrust, 2019) <www.beyondtrust.com/resources/whitepapers/privileged-access-threat-report> accessed 5 May 2020; 'Insider and Third-Party Access Rank as Top Cyber Threats for Global Organisations' (*BeyondTrust*, 9 May 2017) <https://www.beyondtrust.com/press/secure-access-report> accessed July 20, 2020; Robin Kurzer, 'Report: Majority of companies fear 3rd-party vendors make them vulnerable to GDPR legal risks' (*MarTech Today*, 31 July 2018) <https://martechtoday.com/report-majority-of-companies-fear-that-3rd-party-vendors-make-them-vulnerable-to-legal-risks-for-gdpr-non-compliance-218922> accessed 1 August 2020.

[247] Ponemon Institute, 'Data Risk in the Third-Party Ecosystem: Third Annual Report' (2018).

[248] ibid., 2, 15.

or stolen by an Nth vendor'.[249] This distrust is heightened in a context where third parties' lax cybersecurity standards are a rising cause of many incidents.[250]

The same study reported that many companies do not oversee their third-parties to an appropriate degree. The number of companies that 'frequently [review] the policies and programs of their third parties to ensure they address the ever-changing landscape of third-party risk and regulations' is as low as 42%.[251] Only 46% affirmed that they 'monitor the security and privacy practices of vendors with whom they share sensitive or confidential information'.[252] Companies 'regularly report to the boards of directors on the effectiveness of their organization's third-party management program and potential risks' in only 39% of cases.[253] The number that 'know how their information is being accessed or processed by Nth parties with whom they have no direct relationship' is remarkably low, at 15%.[254] There is also low performance when it comes to curating a 'comprehensive inventory of all their third parties'.[255] Merely 34% report that they do so.[256] The 'complexity in third-party relationships' and 'a lack of centralized control over the management of third-party relationships' emerged as key issues for why this number is not higher.[257] In addition, a lack of resources inhibits many companies from conducting appropriate third-party oversight.[258] A low dedication to oversight only further exacerbates these issues. These problems are a prime concern for only 46%.[259] It is concerning that this low effort and commitment persists in a cyber landscape that is increasingly vulnerable through third-parties+.

ii. Third-Party+ Oversight in the NIS Directive

The 2020 proposed revision of the NIS Directive strengthens third-party+ oversight by requiring supply chain risk assessments. It stipulates that '[e]ntities should...assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures'.[260] The revised NIS Directive thus looks to facilitate significant improvements in this area. As intimated in the following discussion, and

[249] Ponemon Institute, 'Data Risk in the Third-Party Ecosystem: Third Annual Report' (2018) 2.
[250] ibid.; 'Insider and Third-Party Access Rank as Top Cyber Threats for Global Organisations' (*BeyondTrust*, 9 May 2017) <https://www.beyondtrust.com/press/secure-access-report> accessed July 20, 2020.
[251] Ponemon Institute, 'Data Risk in the Third-Party Ecosystem: Third Annual Report' (2018) 3.
[252] ibid.
[253] Ibid., 2.
[254] ibid., 3, 13.
[255] ibid., 3, 10.
[256] ibid.
[257] ibid.
[258] ibid., 2, 8.
[259] ibid., 2.
[260] NIS Directive II 21.

considered further in Section IV.II., however, more can be done in this area, particularly in relation to the GDPR.

iii. Third-Party+ Oversight in GDPR

Articles 4, 24, and 28 of the General Data Protection Regulation (GDPR) address controllers and processors and specify their general responsibilities (see Sub-Section II.ix.).[261] Under current regulations, the controller is responsible for making sure its processors have the competency to process personal data in line with the GDPR.[262] The supervisor can take disciplinary action against both the controller and the processor if they do not fulfil their respective obligations.[263] Although a processor is liable for its lapses, it is the controller who is ultimately supposed to ensure that it, its primary processors, and its third-party+ processors comply with the GDPR.[264] The controller is liable to corrective measures and administrative fines for lapses on the part of its processors.[265]

However, after a legal authority has forced a controller to compensate a data subject, the controller can 'claim back' some compensation from relevant processors (or other controllers).[266] This provision's intent is to sanction processors (and other controllers) that mismanage data. However, this provision may also unintentionally weaken the incentive for controllers to police their processors' data protection practices.

Article 82(5) states:

> Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that

[261] Carla Bouca, 'EU GDPR Controller Vs. Processor – The Differences' (*Advisera Expert Solutions Ltd.,* 2020) <https://advisera.com/eugdpracademy/knowledgebase/eu-gdpr-controller-vs-processor-what-are-the-differences/> accessed 27 February 2020.
[262] GDPR Art. 5(2), Art. 24, Art. 28.
[263] GDPR Art. 58, Art. 83.
[264] GDPR Art. 5(2), Art. 24, Art. 28.
[265] Carla Bouca, 'EU GDPR Controller vs. Processor – The Differences' (*Advisera Expert Solutions Ltd.,* 2020) <https://advisera.com/eugdpracademy/knowledgebase/eu-gdpr-controller-vs-processor-what-are-the-differences/> accessed 27 February 2020; 'What Responsibilities and Liabilities Do Controllers Have When Using A Processor?' (*Information Commissioner's Office*, 2019) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/responsibilities-and-liabilities-for-controllers-using-a-processor/> accessed 27 February 2020.
[266] GDPR Art. 82(5).

> part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

According to paragraph 4:

> Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

According to paragraph 2:

> Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

Since a processor can be held responsible if it 'has acted outside or contrary to lawful instructions of the controller'[267], and the controller can get compensation from the processor on that basis, the pressure for controllers to issue lawful instructions as a product of high-quality rather than low-quality oversight on their part is not as high as it might otherwise be. There thus exists a slight tension between the stipulation that controllers have prime responsibility for oversight and their ability to seek compensation from processors for lapses that higher-quality oversight on the controller's part might have avoided.

iv. Mitigation in the Financial Sector

The issues highlighted in Sub-Section III.II.i. are expected to see significant mitigation in the financial sector through the 24 September 2020 proposal on 'digital operational resilience for the financial sector'. These measures include 1) more stringent oversight requirements for financial institutions with respect to critical ICT third-party service providers, 2) the establishment of an Oversight Forum and a Lead Overseer to assist financial institutions with the supervision of critical third-parties, as well as 3) oversight fees to be paid to the European Supervisory

[267] GDPR Art. 82(2).

Authorities (ESAs) by the third-party in exchange for the ESAs reducing the third-party's burdens with respect to conducting inspections themselves.[268]

The proposal asserts that financial entities 'shall at all times remain fully responsible for complying with, and the discharge of, all obligations under this Regulation and applicable financial services legislation'.[269] As with the GDPR's allocation of responsibility to controllers, however, this assertion can potentially be somewhat undermined by the GDPR allowing the controller to retroactively gain compensation from the processor. While this is less of an issue with respect to the oversight of critical third-party service providers—given the stringent oversight that the Oversight Forum and Lead Overseer would provide—the issue may still be relevant for controllers that are sub-contractors of that third-party, notwithstanding financial institutions' responsibilities to assess the supply chain of their critical third-party contractors. In addition, addressing this issue outside of the financial sector has a bearing on financial cybersecurity, in so far as hybrid incidents that involve third-party+ vendors in other sectors of the economy impact the financial system.

[268] Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 2020/0266 (COD) Chapter V.
[269] ibid., Art. 25.

III.III. ZERO-DAY VULNERABILITIES

Zero-day vulnerabilities are significant security risks. They refer to newly discovered flaws in software programmes or operating systems. Developers effectively have 'zero days' to fix the issue, since the running system is already flawed.[270] Zero-day attacks occur when a system provider fails to release a patch before hackers exploit the security flaw. 'Black hat' hackers are groups or individuals who make a profit by discovering and exploiting zero-day vulnerabilities.[271] Some actors, including some governments, pay or actively look for these vulnerabilities.[272] In some cases, an actor will use this information to launch a concerted cyberattack. In others, they utilise vulnerabilities for criminal investigations, espionage, or the development of defence mechanisms.[273] It is conceivable that entities—whether individuals, non-state actors, or governments—that are intent on cyber warfare or terrorism can collect enough vulnerabilities in critical sectors to cause systemic instability.[274] Cyber vulnerabilities thus pose a significant security threat to financial systems.

Even when entities do not use vulnerabilities for overt disruption or security researchers seek to inform a system provider about a vulnerability in good faith, vulnerability discovery, collection, or reporting outside appropriate disclosure policies can endanger a system provider's cybersecurity. Appropriate coordinated vulnerability disclosure (CVD) policies for researching, patching, and disclosing vulnerabilities are a vital cybersecurity issue that this section addresses.

This section begins by outlining the WannaCry and NotPetya attacks, which illustrate the general importance of early vulnerability disclosure and rapid patching of all affected systems. This outline is followed by an overview of CVD in the EU. This section concludes by highlighting the issue that is pursued further in Section IV.III., namely that of fostering the widespread development of rigorous CVD policies in contexts where CVD development is, to a significant extent, shaped at company-level.

---

[270] 'Zero-Day Vulnerability: What it is, and How it Works' (*Norton*) <https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html> accessed 10 March 2020.
[271] Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) i.
[272] ibid.
[273] Sven Herpig and Ari Schwartz, 'The Future of Vulnerabilities Equities Processes Around the World (*Lawfare Institute*, 4 January 2019) <www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world> accessed 13 March 2020.
[274] Greg Ros, 'The Making of a Cyber Crash: a Conceptual Model for Systemic Risk in the Financial Sector' (*ESRB,* 2020) 10-12, 23-24.

i. WannaCry, NotPetya, and Zero-Day Vulnerabilities

The WannaCry and NotPetya attacks indicate the importance of identifying, reporting, and handling zero-day vulnerabilities before an attack can occur. The former affected the UK's National Health Service (NHS) online systems in May 2017. The ransomware exploited a vulnerability in the Microsoft Windows Operating System and encrypted the files on PC hard drives. This breached patients' data and affected access to it.[275] The attackers demanded a bitcoin ransom in exchange for the files. The incident led to cancelled appointments and aborted surgeries in NHS hospitals. A month later, the NotPetya attacks exploited the same vulnerability, to first cripple systems in Ukraine before proliferating internationally with unprecedented speed.

The 2017 WannaCry and NotPetya attacks heightened discussions about appropriate disclosure processes. Controversy surrounds the US National Security Agency's delayed disclosure of software vulnerabilities that it discovered in Microsoft's system.[276] The NSA warned Microsoft only after malicious actors stole the NSA's Eternal Blue hacking programme, which exploits the vulnerability. By that time, the NSA had known about the vulnerability for several years. Microsoft was able to develop a patch before the WannaCry and NotPetya attacks, but not all system users downloaded the patch in time.

Inconsistent patch implementation and the NSA's slow vulnerability disclosure were, thus, two factors that facilitated WannaCry and NotPetya.[277] Some commentators emphasise the role of the former while others emphasise the latter. While the NSA warned Microsoft in time for them to develop a patch two months in advance of the attack, some commentators argue that the NSA's slow disclosure critically reduced the timeline in which a patch could be developed and

[275] 'NHS Cyber-Attack: GPs and Hospitals Hit by Ransomware' (*BBC,* 13 May 2017) <https://www.bbc.com/news/health-39899646> accessed 22 March 2020.
[276] ibid., Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History' (*Wired,* 22 August 2018) <www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> accessed 21 May 2020; Andy Greenberg, 'The Shadow Broker Mess Is What Happens When the NSA Hoards Zero-Days' (*Wired,* 17 August 2016) <www.wired.com/2016/08/shadow-brokers-mess-happens-nsa-hoards-zero-days/> accessed 1 July 2020; Lily Hay Newman, 'The Leaked NSA Spy Tool That Hacked the World' (*Wired,* 7 March 2018) <www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/> accessed 12 June 2020; Brad Smith, 'The Need for Urgent Collective Action to Keep People Safe Online: Lesson's from Last Week's Attack' (*Microsoft,* 14 May 2017) accessed 1 August 2020; Sven Herpig and Ari Schwartz, 'The Future of Vulnerabilities Equities Processes Around the World (*Lawfare Institute*, 4 January 2019) <www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world> accessed 13 March 2020.
[277] See above; Erik Silfversten, et al. *Economics of Vulnerability Disclosure* (*ENISA,* 2018) 56-57; Ellen Nakashima, 'NSA Found a Aangerous Microsoft Software Flaw and Alerted the Firm—Rather than Weaponizing it' (*The Washington Post*, 14 January 2020) <www.washingtonpost.com/national-security/nsa-found-a-dangerous-microsoft-software-flaw-and-alerted-the-firm--rather-than-weaponize-it/2020/01/14/f024c926-3679-11ea-bb7b-265f4554af6d_story.html> accessed 20 September 2020.

implemented.[278] The NSA example illustrates the importance of speed when addressing zero-day vulnerabilities.

Critique about the NSA's delayed disclosure centres around government disclosure decision processes (GDDP). GDDPs are a category of disclosure processes for which it is legitimate to weigh the security benefits of rapid disclosure against any national security benefits of temporarily withholding information.[279] GDDPs are a government's 'policies and practices to assess the risks and interests associated with disclosing a vulnerability immediately to the affected vendor(s) and/or manufacturer(s) or whether to delay disclosure'.[280] As of the 2018 CEPS report on software vulnerability disclosure, many member states have not yet implemented a GDDP.[281] A CEPS Task Force suggests that in addition to supporting member states in their respective CVD implementation, ENISA can share best practices on GDDP.[282]

While more EU member state governments should develop GDDPs[283], GDDPs are not the primary focus of the following discussion. Rather, the NSA-WannaCry-NotPetya example is given to illustrate the magnitude of attacks that zero-day vulnerabilities can cause. The following discussion and its proceeding suggestions, in Section IV.III., focus on CVD, which is a crucial component of GDDPs. For governments with GDDPs, CVD is what kicks in after a choice to disclose has been made.[284] Beyond government entities, an organisation's CVD policy is a security researcher's first point of reference. This section, and Section IV.III., thus focuses on further fostering of the development of strong CVD policies by organisations in the EU.

ii. Security Researchers and Coordinated Vulnerability Disclosure

'White hat' hackers—commonly called security researchers—are individuals or organisations who look for vulnerabilities in software systems to report them to the affected vendor so that the vendor can patch the vulnerability. In some cases, this may involve highlighting the vulnerability

[278] Lily Hay Newman, 'The Leaked NSA Spy Tool That Hacked the World' (*Wired,* 7 March 2018) <www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/> accessed 12 June 2020; Brad Smith, 'The Need for Urgent Collective Action to Keep People Safe Online: Lesson's from Last Week's Attack' (*Microsoft,* 14 May 2017) accessed 1 August 2020.
[279] Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) 61-78.
[280] ibid., 63.
[281] ibid., 73.
[282] ibid., 73-74.
[283] ibid.
[284] ibid., 63.

by downloading data (without effecting irreversible damage).[285] Subsequently sharing vulnerability information with vendors that might have similar vulnerabilities is a crucial way of strengthening cybersecurity.

However, the relationship between security researchers and vendors with vulnerabilities can be contentious, especially if a clear policy for how vulnerabilities should be reported and handled is absent. Tension between researchers and vendors can be a result of an organisation's 'lack of awareness or understanding', 'costs of implementation and operation', 'lack of management support', 'lack of organisational or technical capacity', 'fear of reputational damage or attack', as well as any 'legal barriers or uncertainty'.[286] In addition, 'lack of appropriate vulnerability disclosure avenues', 'insufficient or slow vendor or coordinator communication', and 'fear of hostility or punishment' may cause concern on the reporter's side.[287]

iii. Frameworks for CVD in Europe

CVD policies can mitigate that tension. CVDs are frameworks by which security researchers can alert system providers of software vulnerabilities.[288] They also determine the extent to which other system providers or the wider public will receive information about a vulnerability.[289] Vendors tend to have considerable freedom about whether they adopt a CVD policy and what form that policy takes.[290] In some frameworks, the security researcher contacts the vendor directly.[291] In others, researchers can report to a national CSIRT or other independent party that serves as an intermediary between the reporter and the affected vendor.[292]

Vulnerability discovery, disclosure, patching, and liability have been unevenly regulated in the EU over the past decade. Governments have frequently left such competencies to the private

[285] Rickey Gevers et al., 'Coordinated Vulnerability Disclosure: The Guideline' (*National Cyber Security Centre NL, Ministry of Justice and Security,* 2019) 22.
[286] Erik Silfversten, et al. *Economics of Vulnerability Disclosure* (*ENISA,* 2018) 34, 37.
[287] ibid., 28.
[288] Sven Herpig and Ari Schwartz, 'The Future of Vulnerabilities Equities Processes Around the World (*Lawfare Institute*, 4 January 2019) <www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world> accessed 13 March 2020; Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History' (*Wired,* 22 August 2018) <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> accessed 21 May 2020.
[289] 'Coordinated Vulnerability Disclosure' (*Microsoft Security Response Center*) <https://www.microsoft.com/en-us/msrc/cvd> accessed 24 April 2020; A D Householder, G Wassermann, A Manion, and C King, 'The CERT® Guide to Coordinated Vulnerability Disclosure' (*Software Engineering Institute*, 2017) vii.
[290] Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) 13-40.
[291] Erik Silfversten, et al. *Economics of Vulnerability Disclosure* (*ENISA,* 2018) 13.
[292] ibid., 6, 13.

sector. Some private-sector companies test cybersecurity products for vulnerabilities.[293] There are also live cyber threat maps that keep customers informed of ongoing threats throughout the world.[294] As discussed further below, individual vendors have tended to have significant freedom about whether or not to adopt a CVD policy and how to shape it.

While some member states regulate CVDs at the national level, many do not. The CEPS Task Force on Software Vulnerability Disclosure notes that, as of 2018, only the Netherlands and France have general national CVD policies, with Lithuania having a national policy for CVD in the 'providers of communications networks' sector.[295] There are some efforts to develop national CVD policies in Austria, Belgium, Czechia, Finland, Germany, Italy, Latvia, Luxembourg, Romania, Slovenia, North Macedonia, and the United Kingdom.[296] However, national CVD policies have been largely absent in other member states over the past decade.

At the global level, the International Organization for Standardization (ISO) has published standards for security arrangements in organisations. Standard 27002 provides best practices and management guidelines for data security.[297] The ISO has also introduced two standards for revealing vulnerabilities and handling vulnerability reports.[298] ISO 29147 offers recommendations for vulnerability disclosure. ISO 30111 deals with how to process this sensitive information and gives pointers on how to contain such vulnerabilities. While these serve as baseline data security standards on which governments can build national CVD policies, these standards do not cover the specifics of establishing CVD policies at the national level.[299]

[293] 'What We Do' (*NSS Labs*) <www.nsslabs.com/tested-technologies/threat-detection-analytics-tda/> accessed 20 September 2020; 'Vulnerability Scan in Kaspersky Total Security' (*Kaspersky*) <https://support.kaspersky.com/11474 > accessed 20 September 2020.

[294] 'Live Cyber Threat Map' (*Check Point Software Technologies Ltd,* updated continuously) <https://threatmap.checkpoint.com/> accessed 22 September 2020; 'FireEye Cyber Threat Map' (*FireEye*, updated continuously) <www.fireeye.com/cyber-map/threat-map.html> accessed 23 September 2020; 'Cyber Threat Real-Time Map' (Kaspersky, updated continuously) <https://cybermap.kaspersky.com/> accessed 23 September 2020.

[295] Erik Silfversten, et al. *Economics of Vulnerability Disclosure* (*ENISA,* 2018) 39; Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) i, 13-23.

[296] Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) 13-23.

[297] CIO Experience Group Information Security, 'Coordinated Vulnerability Disclosure: Model Policy and Procedure' (*CIO Platform Nederland: CEG Information Security*, 2016) 11.

[298] ibid.

[299] Allen D. Householder, Garret Wassermann, Art Manion, and Chris King, 'The CERT® Guide to Coordinated Vulnerability Disclosure', (*Software Engineering Institute*, 2017) 29-30

Calls for Harmonisation

There have been a number of calls for CVD harmonisation across the EU.[300] ENISA recommends the Dutch national guidelines as a model for other member states.[301] The 2018 CEPS Task Force likewise endorses the Dutch national framework and additionally points to developments in the US.[302] Representatives from the Joint Research Centre also suggested, at the 2017 CEPS Workshop on Software Vulnerability Disclosure, that there was more to be done at the EU-level.[303] There has thus been a recognised need to develop a coherent and more effective approach to CVD in the interest of cybersecurity.

The Commission's 16 December 2020 proposed revision of the NIS Directive is the first major regulatory step at the EU-level to enhance CVD throughout the union.[304] The revision states that a CSIRT per country will act as a 'coordinator for the purpose of coordinated vulnerability disclosure'.[305] This involves 'facilitating, where necessary, the interaction between the reporting entity and the manufacturer or provider of ICT products or ICT services'.[306] These national CVD coordinators are to work closely with the CSIRTs Network where appropriate.[307] At the EU-level, a proposed European vulnerability registry run by ENISA is to handle the following:

> ...information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches,

[300] Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) iv.
[301] 'Coordinated Vulnerability Disclosure: Guidelines Published by the NCSC', (*ENISA,* 2018) <https://www.enisa.europa.eu/news/member-states/coordinated-vulnerability-disclosure-guidelines-published-by-ncsc> accessed 3 May 2020; William Phillips, Giacomo Persi Paoli, Cosmin Ciobanu, *Economics of vulnerability disclosure*, (*ENISA*, 2018) 39-41.
[302] Erik Silfversten, et al. *Economics of Vulnerability Disclosure*, (*ENISA*, 2018); Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) 23-39.
[303] Ignacio Sanchez and Laurent Beslay, 'EU Zero-Day Vulnerability Management: Challenges and Opportunities to Improve the Security and Resilience of the Digital Single Market', presentation at the CEPS Workshop on Software Vulnerability Disclosure: The European Landscape (Brussels, 23 June 2017); Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) 3.
[304] Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) 53; CERT Capability Team, 'Good Practice Guide on Vulnerability Disclosure: From challenges to recommendations' (*ENISA*, 2015) 70; NIS Directive II Art. 6.
[305] NIS Directive II Art. 6.
[306] ibid.
[307] ibid.

> guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated.[308]

This information would be available to 'all interested parties'.[309]

iv. Need for Rigorous CVD Policies in the Private Sector

Both of these national and EU-level frameworks will significantly strengthen CVD in the EU by clarifying the bases by which security researchers and affected vendors can and should operate with respect to CVD. However, while ENISA and the national CVD coordinators can be expected to provide guidelines about CVD, the particulars of any given CVD policy are, to a significant extent, at the discretion of the individual vendors.[310] This follows the widely accepted rationale that 'no one size fits all'.[311]

Therefore, a significant issue is how to foster the implementation of robust CVD at company level, given the additional lack of *ex-ante* supervision for 'important entities' as per the Commission's proposed revision of the NIS Directive.[312]

NIS Directive, Ex Post Supervision, and CVD

The revised directive stipulates that 'essential entities should be subject to a fully-fledged supervisory regime (*ex-ante* and *ex-post*), while important entities should be subject to a light supervisory regime, *ex-post* only'. On the one hand, this is a stronger approach to supervision compared to the initial NIS Directive, which stipulates *ex post* supervision without distinction between essential and important entities. The revised draft thus significantly strengthens the supervision of essential entities. On the other hand, there is still room for mitigating issues associated with *ex post* supervision with respect to important entities. The draft states...

> ...that important entities should not document systematically compliance with cybersecurity risk management requirements, while competent authorities should

[308] NIS Directive II Art. 6.
[309] ibid.
[310] ibid., 19, Art. 10(4)(c).
[311] Allen D. Householder, Garret Wassermann, Art Manion, and Chris King, 'The CERT® Guide to Coordinated Vulnerability Disclosure', (*Software Engineering Institute*, 2017) 29-30; Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) 37-38; NIS Directive II 19, Art. 10(4)(c).
[312] NIS Directive II 27.

> implement a reactive *ex-post* approach to supervision and, hence, not have a general obligation to supervise those entities.[313]

While there are many benefits to the *ex post* supervisory approach—and CVD regulations that incorporate *ex post* supervision should be adopted throughout the EU—an *ex post*-only approach is vulnerable to information asymmetry between vendors and supervisors concerning a vendor's compliance.[314] Vendors can sometimes take advantage of this information asymmetry and be uncompliant.[315]

The discussion in Section IV.III. therefore considers possible private sector initiatives that uphold the 'no one-size-fits-all' principle while establishing common standards.

v. The Issue of Wider Disclosure

The exact dynamics of how much, by when, and by whom information should be shared with a wider audience are often a matter of discretion and discussion between a vendor and the discoverer.[316] Although completely refusing to share information about vulnerabilities is against the generally-expected norm, it is conceivable that a vendor might refuse to share information, and even pressure the discoverer to keep quiet, in order to mitigate negative security or reputational repercussions.[317] Even where national and sectoral CVD frameworks exist, a general expectation of disclosure is not always accompanied by an absolute requirement.[318] While the revised NIS Directive encourages and facilitates wider vulnerability disclosure through the vulnerability repository, as well as through national CVD coordinators that would help with 'negotiating disclosure timelines', submitting information to the repository for wider disclosure would be voluntary.[319]

The Commission's proposed regulation on 'digital operational resilience for the financial sector' looks to strengthen the vulnerability information sharing framework for the financial sector. Article 13 states that 'financial entities shall have in place communication plans enabling a

[313] NIS Directive II 27.
[314] Sven Hoeppner and Christian Kircher, 'Ex Ante Versus Ex Post Governance: A Behavioral Perspective' [2016] 12(2) RLE 227-230.
[315] ibid.
[316] William Phillips, Giacomo Persi Paoli, Cosmin Ciobanu, *Economics of Vulnerability Disclosure*, (*ENISA*, 2018) 33-39.
[317] ibid.; 'Experts Letter on the Importance of Security Research' (*Center For Democracy* & Technology, 10 April 2018) <https://cdt.org/insights/experts-letter-on-the-importance-of-security-research/> accessed 1 November 2020.
[318] William Phillips, Giacomo Persi Paoli, Cosmin Ciobanu, *Economics of Vulnerability Disclosure*, (*ENISA*, 2018) 33-39.
[319] NIS Directive II 19, Art. 6.

responsible disclosure of ICT-related incidents or major vulnerabilities to clients and counterparts as well as to the public, as appropriate'.[320] The draft regulation also states that 'the ESAs should share anonymised data on threats and vulnerabilities relating to an event to aid wider collective defence'. [321] These stipulations would further facilitate wider vulnerability information sharing with relevant parties, but there is more to be discussed about how much and by when vendors should share information with relevant coordinators and other vendors.

In an integrated financial system like the Eurozone, rapid information sharing about vulnerabilities is an important cybersecurity tool. If a vulnerability is a particularly sensitive and widespread one, other vendors that do not know that they have similar vulnerabilities may be compromised if those in the know take a long time to disseminate information about the vulnerability. There is also the possibility that the first contacted vendor is uncommunicative upon receiving a report.[322] While these issues are mitigated by the recently drafted stipulations for CVD in the financial sector, they may still be relevant elsewhere, particularly when they affect entities in other sectors that may, in turn, affect financial stability.

[320] Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 COM(2020) 595 final Art. 13.
[321] ibid., 21.
[322] 'CISA Coordinated Vulnerability Disclosure (CVD) Process' (*Cybersecurity and Infrastructure Security Agency, Department of Homeland Security,* 3 December 2019) <www.cisa.gov/coordinated-vulnerability-disclosure-process> accessed 28 April 2020.

III.IV. THE RELATIONSHIP BETWEEN LAW AND TECH

Reducing disjunction between regulation and technology is important for cybersecurity. Financial systems are connected by diverse technologies that are often built without full knowledge of the systems with which they interface.[323] Technical vulnerabilities at system interfaces are exacerbated if some technologies do not (or cannot) comply fully with security regulations. Where diverse technologies in a system vary in their compliance with security regulations, the risk of a vulnerability going undetected and contributing to systemic risk is much higher. Disjunction and fragmentation across jurisdictions in highly-integrated networks further exacerbate cyber risk.

Emerging technologies pose a particular challenge to regulators. Many of their characteristics have no precedent. For both regulators and fintech companies, it is sometimes difficult to determine which aspects of an emerging technology correspond to a given requirement. For example, the EU's GDPR requires some entities to be categorised as controllers and others as processors, to help determine who is responsible for areas of a system's cybersecurity in terms of data protection (see Sub-Section II.ix.). As discussed further in Section III.V., however, it is challenging to identify controllers and processors in decentralised technologies, like, for example, blockchain. In other words, it is difficult to identify, report, and engage with parties responsible for aspects of a decentralised system's cybersecurity. There is a disjunction here between regulation and technology that has the potential to impact cybersecurity.

There is considerable debate about how gaps like this can and should be closed.[324] One perception is that the slow regulatory process lags behind technological progress and needs to be made more agile and forward-looking.[325] On the flip side, there is the argument that most regulations do not suppress innovation. According to this view, it is the private sector's responsibility to meet regulatory security standards.[326]

[323] Claudia Ng, 'Regulating Fintech: Addressing Challenges in Cybersecurity and Data Privacy', (*Harvard Kennedy School,* 22 February 2018) <www.innovations.harvard.edu/blog/regulating-fintech-addressing-challenges-cybersecurity-and-data-privacy> accessed 4 June 2020; ENISA, 'Distributed Ledger Technology & Cybersecurity: Improving Information Security in the Financial Sector' (2016) 7.
[324] Mark D. Fenwick, Wulf A. Kaal, Erik P. M. Vermeulen, 'Regulation Tomorrow: What Happens When Technology Is Faster than the Law?' [2017] American University Business Law Review 6(3).
[325] Daniel Malan, 'The Law Can't Keep up with New Tech. Here's How to Close the Gap', (*World Economic Forum*, 2018), <https://www.weforum.org/agenda/2018/06/law-too-slow-for-new-tech-how-keep-up/> accessed 10 March 2020.
[326] Lalita Clozel, 'OCC's Curry Rules Out 'Safe Space' for FinTech Companies' (*American Banker*, 3 November 2016).

One middle ground view is the 'comply or explain' approach to corporate governance found in the EU.[327] According to comply-or-explain, the spirit of the law is given precedence over the letter of the law. It allows entities to substitute the specifics of how they intend to uphold the standards required by a given regulation, as long as they offer a strong case for doing so.

Nevertheless, fintech developers are often uncertain about which regulations are relevant to their product. The existence of multiple regulatory agencies exacerbates regulatory ambiguity.[328] This problem is especially acute at the level of supranational governance.[329]

The Collingridge dilemma expresses part of the difficult relationship between law and emerging tech.[330] It is a practical reality that it is difficult to regulate a technology until it matures. Doing so is challenging because one has insufficient information about a new technology as it is emerging. On the other hand, it is difficult to readjust an already established and mature technology due to technological and stakeholder rigidities.

i. Need for More Frequent Reviews of Cybersecurity Regulation

The EU has a number of mechanisms in place to keep regulations fit for the times and many EU regulations and certification schemes are reviewed on regular cycles. The European Commission's regulatory fitness and performance programme (REFIT) 'aims to make EU laws simpler, more targeted and easier to comply with', wherever possible.[331] However, technology is

[327] Commission Recommendation of 9 April 2014 on the quality of corporate governance reporting ('comply or explain') Text with EEA relevance [2014] OJ L 109; Corporate governance: European Forum clarifies 'comply or explain' principle and issues annual report' (*European Commission,* 6 March 2006) <https://ec.europa.eu/commission/presscorner/detail/en/IP_06_269> accessed 18 September 2020; Directive 2006/46/EC of the European Parliament and of the Council of 14 June 2006 amending Council Directives 78/660/EEC on the annual accounts of certain types of companies, 83/349/EEC on consolidated accounts, 86/635/EEC on the annual accounts and consolidated accounts of banks and other financial institutions and 91/674/EEC on the annual accounts and consolidated accounts of insurance undertakings (Text with EEA relevance) [2006] OJ L 224; Daniel Malan, 'The Law Can't Keep up with New Tech. Here's How to Close the Gap' (*World Economic Forum*, 21 June 2018) <www.weforum.org/agenda/2018/06/law-too-slow-for-new-tech-how-keep-up/> accessed 18 September 2020.

[328] Luke Thomas, 'The Case for Federal Regulatory Sandbox for FinTech Companies' [2018] 22 NC Banking Instit. 278.

[329] ibid.

[330] David Collingridge, *The Social Control of Technology* (Open University Press, 1981); Simone van der Burg 'Co-shaping the Life Story of a Technology: From Technological Ancestry to Visions of the Future' in Simone van der Burg and Tsjalling Swierstra (eds.), *Ethics on the Laboratory Floor* (Palgrave Macmillan, 2013).

[331] 'REFIT – Making EU Law Simpler, Less Costly and Future Proof' (*European Commission*) <https://ec.europa.eu/info/law/law-making-process/evaluating-and-improving-existing-laws/refit-making-eu-law-simpler-less-costly-and-future-proof_en> accessed 1 November 2020.

developing at an ever-increasing pace.[332] It can be questioned whether the pace at which tech develops is adequately accounted for by the review frequency stipulated in many regulations.[333]

Several frameworks relevant to financial cybersecurity are reviewed every four to five years.

- The first review of the Commission's proposed regulation on 'digital operational resilience for the financial sector' (as per Article 51) is expected to be five years following its ratification.
- NIS Directive II (as per Article 35) is to be reviewed 'periodically' on what looks to become a four-and-a-half year review cycle.
- GDPR (as per Article 97) and eIDAS (as per Article 49) are both reviewed every four years.

Frameworks with other review periods include:

- The Commission's proposed regulation on Markets in Crypto-Assets, which would be evaluated three years following its ratification.[334]
- ECB TARGET2, which (as per Article 3.7.8) is reviewed annually and ad hoc, if necessary.
- The 'pilot regime for market infrastructures based on distributed ledger technology', which (as per Article 9(6)) would be evaluated annually by the ESMA with respect to the implementation of 'specific permissions, related exemptions and conditions attached thereto…as well as any compensatory or corrective measures required'. This is in addition to evaluations that the ESMA and the Commission are to conduct within five years.[335]

At present, ENISA uses a five-year re-evaluation cycle for European cybersecurity certification schemes. Within those five years, ENISA collects stakeholder feedback which it uses to inform its evaluations.[336] The usual five-year evaluation cycle thus allows ENISA to cooperate with the

[332] Declan Butler, 'A World Where Everyone Has a Robot: Why 2040 Could Blow your Mind' (*Nature*, 24 February 2016) <www.nature.com/news/a-world-where-everyone-has-a-robot-why-2040-could-blow-your-mind-1.19431> accessed 21 October 2020.
[333] Harriet Barlow, 'The Race to Regulate: Can the Law Keep Pace with Technology Innovation?' (*JDX Consulting,* 8 August 2019) <www.jdxconsulting.com/technology/the-race-to-regulate-can-the-law-keep-pace-with-technology-innovation/> accessed 20 October 2020.
[334] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and amending Directive (EU) 2019/1937 COM(2020) 593 final 151.
[335] Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology COM(2020) 594 final 4.
[336] Cybersecurity Act Art. 49(8).

private sector and provide well-considered advice. ENISA may also review a certification at an earlier stage if the European Commission requests it to do so. There is thus a mechanism for reviewing certification ad hoc where the disjunction between law and technology results in pressing issues. This mechanism tends to be reactive rather than proactive, however.

The issue of how to develop proactive regulatory reviews that are suitable for the pace of technological change is a pertinent one, given the four to five-year cycles stipulated for these frameworks. As indicated above, however, there are benefits to these longer review cycles. The suggestions put forward in Sub-Section IV.IV.i. thus seek to merge the benefits of both approaches.

ii. Regulatory Sandboxing and Its Limited Presence in the EU

Regulatory sandboxing is another way in which regulators and fintech companies can cooperate when an emerging technology seems too complicated to regulate conventionally. Regulatory sandboxing is a relatively recent concept, which was first tried in full by the UK's Financial Conduct Authority (FCA).[337] Regulatory sandboxes allow fintech companies to trial in the market despite not yet being in full compliance with regulations.[338] As indicated above, the nature of any given emerging financial technology may prevent some fintech from entering the market in full compliance with existing regulations. A regulatory sandbox relaxes or adapts regulatory requirements for a certain amount of time under close supervision from the competent authority.

Opponents of regulatory sandboxing are concerned that relaxing regulation will undermine 'consumer protection or safety and soundness'.[339] An extension of this concern is that there might be a 'race to the bottom' for regulatory leniency.[340] However, as a joint report by the European Supervisory Authorities (ESAs) asserts, 'sandboxes do not entail the disapplication of regulatory requirements that must be applied as a result of EU law'.[341] This principle informs all existing

[337] 'The First Cohort of the First Fintech Regulatory Sandbox' (*BBVA*, 28 May 2018) <www.bbva.com/en/first-cohort-first-fintech-regulatory-sandbox/> accessed 1 September 2020.
[338] Luke Thomas, 'The Case for Federal Regulatory Sandbox for FinTech Companies' [2018] 22 NC Banking Instit. 271.
[339] ibid., 268-269
[340] ibid., 278.
[341] European Securities and Markets Authorities, European Banking Authority, European Insurance and Occupational Pensions Authority, 'Report—FinTech: Regulatory sandboxes and innovation hubs' [2018] JC 74 16.

sandboxes in EU member states.[342] Retaining high consumer protection standards is integral to the sandbox idea.[343]

One way by which authorities can relax regulations without undermining consumer protection and cybersecurity is by removing the threat of federal fines without lowering consumer compensation requirements.[344] This approach will motivate fintech companies to meet consumer protection requirements, even if they do so in unconventional ways that are better suited to the nature of their emerging tech. Under the competent authority's supervision, and in compliance with transparency requirements, fintech in regulatory sandboxes must still fulfil the spirit of consumer protection and cybersecurity regulation even if the emerging nature of the technology does not make it feasible to meet the existing letter of the law.[345]

To qualify for a regulatory sandbox in the Netherlands, for example, a fintech company needs to be able to show that it 'cannot reasonably' adhere to the particulars of existing regulation but has a plan for how it can comply with the spirit of the regulation.[346] Using blockchain as an example, the De Nederlandsche Bank states that a fintech company must show 'that it meets the aim of sound and ethical operational management using blockchain technology, in a different but more efficient and better way'.[347] The fintech's operations need to be transparent and not endanger '[t]he solidity of financial services companies and the stability of the financial system'.[348] Regulatory sandboxes in Denmark, Lithuania, and the UK make it a key point to consider the extent to which a given fintech will 'offer identifiable customer benefits'.[349] The common standard in member countries with sandboxes is that the fintech company has to demonstrate clear 'readiness' to enter a live market environment.[350] Such initiatives strike a key balance between

[342] European Securities and Markets Authorities, European Banking Authority, European Insurance and Occupational Pensions Authority, 'Report—FinTech: Regulatory sandboxes and innovation hubs' [2018] JC 74 17-18.
[343] Luke Thomas, 'The Case for Federal Regulatory Sandbox for FinTech Companies' [2018] 22 NC Banking Instit. 278.
[344] Brian Knight, 'Innovation Will Stall Without a Regulatory Fintech 'Sandbox'', (*American Banker*, 15 November 2016) <https://www.americanbanker.com/opinion/innovation-will-stall-without-a-regulatory-fintech-sandbox> accessed 7 June 2020.
[345] Luke Thomas, 'The Case for Federal Regulatory Sandbox for FinTech Companies' [2018] 22 NC Banking Instit. 272, 278.
[346] De Nederlandsche Bank and AFM, 'More Room for Innovation in the Financial Sector: Market Access, Authorisations and Supervision—Next Steps *AFM—DNB*' (2016) 3.
[347] ibid., 3
[348] ibid.
[349] European Securities and Markets Authorities, European Banking Authority, European Insurance and Occupational Pensions Authority, 'Report—FinTech: Regulatory Sandboxes and Innovation Hubs' [2018] JC 74 23.
[350] ibid., 22-24.

encouraging innovation within the financial sector and protecting the overall health of the wider financial system. The aforementioned concerns can thus be effectively mitigated.

Few EU Member States with Regulatory Sandboxes

In light of the above, the relationship between emerging financial technologies and regulation could be significantly strengthened by the implementation of regulatory sandbox frameworks throughout the EU. While extant in some EU member states, regulatory sandboxing is not widespread. At present, EU members with live regulatory sandboxes include only the UK, Denmark, Lithuania, Poland, Malta, and the Netherlands.[351] Norway has announced a regulatory sandbox scheme, Spain has a draft bill, and Hungary is looking into the possibility.[352]

The Issue of Sandbox Coherence between Member States

The proliferation of regulatory sandboxes throughout the EU could do much to improve the relationship between law and tech. However, any initiatives to that effect must take the issues of fragmentation and sandbox diversity into account. Sandboxing initiatives for inter-jurisdictional fintech will have limited effectiveness if there is significant variation in sandboxing frameworks across the EU. This problem has arisen in the US, where no federal regulatory sandbox exists. Instead, there are twelve federal regulatory agencies and approaches vary significantly across states.[353] A fragmented approach to fintech sandboxing in a highly integrated financial region like the EU will reduce the benefits of sandboxing since the fragmentation will make it difficult for a fintech to operate smoothly across borders.[354] It is important to either have similar regulatory sandboxing frameworks between member states or one that sets a supranational standard.[355]

An EU-level Regulatory Sandbox

An EU-level regulatory sandbox has yet to be implemented. While the European Council's 16 November 2020 conclusions indicate that 'a pan-European blockchain regulatory sandbox' is in development for implementation in 2021/2022, EU-level regulatory sandboxing pends further

[351] 'Regulatory Sandboxes', (*Columbia Business School: The Columbia Institute for Tele-information*, 2016) <https://dfsobservatory.com/content/regulatory-sandboxes> accessed 4 June 2020.
[352] European Securities and Markets Authorities, European Banking Authority, European Insurance and Occupational Pensions Authority, 'Report—FinTech: Regulatory Sandboxes and Innovation Hubs' [2018] JC 74 16-17.
[353] Luke Thomas, 'The Case for Federal Regulatory Sandbox for FinTech Companies' [2018] 22 NC Banking Instit. 272.
[354] ibid.
[355] European Securities and Markets Authorities, European Banking Authority, European Insurance and Occupational Pensions Authority, 'Report—FinTech: Regulatory Sandboxes and Innovation Hubs' [2018] JC 74 37-39.

consideration by the Commission.[356] On the whole, the Council views regulatory sandboxing favourably and has put forward a timeline for efforts to strengthen sandboxing in the EU.[357] The Council asks the Commission 'to evaluate the use of experimentation clauses in ex-post evaluations and fitness checks on the basis of an exchange of information with member states' by mid-2021.[358] The Council also tasks the Commission with undertaking an initial draft of 'practical recommendations on the possible future use of regulatory sandboxes and experimentation clauses in the EU and at EU level' by the end of 2021.[359]

* * *

Sub-Section IV.IV.ii. of this paper discusses how a multi-sectoral, EU-level regulatory sandboxing framework might look like and puts forward suggestions on the subject. In so far as an EU-level regulatory sandbox for a given sector is yet to be established, Sub-Section IV.IV.ii. emphasises the importance of harmonisation between member state frameworks.

[356] General Secretariat of the Council, 'Council Conclusions on Regulatory Sandboxes And Experimentation Clauses As Tools For An Innovation-Friendly, Future-Proof And Resilient Regulatory Framework That Masters Disruptive Challenges In The Digital Age' [2020] 13026/20 4-5; 'ECB Announces Support for FintechBank Applicants' (*Lantham & Watkins LLP*, 20 November 2017), <www.latham.london/2017/11/ecb-announces-support-for-fintech-bank-applicants> accessed 1 June 2020.
[357] 'Regulatory Sandboxes and Experimentation Clauses as Tools for Better Regulation: Council Adopts Conclusions' (*The European Council*, 16 November 2020), <www.consilium.europa.eu/en/press/press-releases/2020/11/16/regulatory-sandboxes-and-experimentation-clauses-as-tools-for-better-regulation-council-adopts-conclusions/> accessed 16 November 2020.
[358] ibid.
[359] General Secretariat of the Council, 'Council Conclusions on Regulatory Sandboxes And Experimentation Clauses As Tools For An Innovation-Friendly, Future-Proof And Resilient Regulatory Framework That Masters Disruptive Challenges In The Digital Age' [2020] 13026/20 5.

III.V. BLOCKCHAIN, SECURITY, AND THE FINANCIAL SYSTEM

This section addresses one particular emerging technology that has become increasingly relevant to the financial industry in recent years: blockchain. Blockchain technology is an 'append-only' database (i.e., there are no provisions to alter or delete previous records). In such a database, transactions are grouped as a series of 'blocks'. Each appended block in a given network can contain up to a specific number of transactions, which affects the network's transaction rate. Bitcoin's rate is three to seven transactions per second while Ethereum's is fifteen.[360]

Decentralised technologies like blockchain are now being utilised by some global security exchanges.[361] Some financial firms have started to explore the possibilities for integrating blockchain into more mainstream financial systems. As mainstream financial institutions increasingly experiment with blockchain's capabilities,[362] gaps or grey-zones between existing regulations and emerging technologies will only become more pertinent to financial cybersecurity.

On the whole, blockchain is a growing presence in the EU. Although most production-level initiatives and platforms are still in their infancy, the rapid development of blockchain indicates that its presence and applicability will only continue to grow.[363] The past four years have seen a rapid move from proofs-of-concept, to large-scale project development, and to the implementation of those projects.[364]

The decentralised community of blockchain developers and users is a growing one. Now stakeholders are beginning to turn their thoughts towards more concerted approaches to decentralised technologies.[365] If nascent initiatives are anything to go by, greater consolidation of the blockchain landscape can be expected in the future.[366]

---

[360] Turner Wright, 'Ethereum Now Rivals Bitcoin for Daily Value Transfers' (*Cointelegraph*, 16 April 2020) <https://cointelegraph.com/news/ethereum-now-rivals-bitcoin-for-daily-value-transfers> accessed 10 September 2020; 'Transaction Rate Per Second' (*Blockchain*) <www.blockchain.com/charts/transactions-per-second> accessed 20 December 2020.

[361] How the Blockchain Will Impact the Financial Sector (*Knowledge@Wharton* 16 November 2018) <https://knowledge.wharton.upenn.edu/article/blockchain-will-impact-financial-sector/> accessed 10 September 2020.

[362] ibid.

[363] Tom Lyons, Ludovic Courcelas, and Ken Timsit, 'Scalability, Interoperability, and Sustainability of Blockchains (*EBOF*, 2019).

[364] ibid.

[365] Ludovic Courcelas, Tom Lyons, and Ken Timsit, 'The EU Blockchain Observatory and Forum, Conclusions and Reflections 2018-2020 (*EBOF*, 2020).

[366] ibid.

Recent Regulatory Initiatives

Significant strides in this direction include the Financial Action Task Force (FATF) Travel Rule and the European Commission's 24 September 2020 proposals for regulation on Markets in Crypto-Assets and regulation on 'a pilot regime for market infrastructures based on distributed ledger technology'.[367] The first concerns the use of Virtual Asset Service Providers (VASPs) to identify the 'originator' and 'beneficiary' of cryptocurrency transfers.[368] The second aims to strengthen and harmonise 'transparency and disclosure', 'authorisation and supervision', 'operation, organisation and governance', 'consumer protection rules', and 'measures to prevent market abuse' with respect to many virtual assets.[369] The third 'lays down requirements on multilateral trading facilities and securities settlement systems using distributed ledger technology "DLT market infrastructures"'.[370] These requirements pertain to '(a) granting and withdrawing...specific permissions', '(b) granting, modifying and withdrawing related exemptions', '(c) mandating, modifying and withdrawing attached conditions, compensatory or corrective measures', '(d) operating such DLT market infrastructures', '(e) supervising such DLT market infrastructures', and '(f) cooperation between operators of DLT market infrastructures, competent authorities and ESMA'.[371] ESMA would act as a point of contact for incident reports and serve as a coordinator towards competent authorities on matters relating to DLT, particularly supervision.[372]

While these measures significantly strengthen the security standards for virtual assets, particularly decentralised financial technologies, the regulation of this area is still nascent and experimental. The expressed purpose of the proposed regulation on the 'pilot regime for market infrastructures based on distributed ledger technology' is 'the experimentation of DLT market infrastructures' and 'allowing supervisors and legislators to identify obstacles in the regulation, while regulators

[367] FATF, '12-Month Review Of The Revised FATF Standards On Virtual Assets And Virtual Asset Service Providers' (FATF, 2020) <www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html> accessed 06 November 2020; Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and amending Directive (EU) 2019/1937 COM(2020) 593 final; Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology COM(2020) 594 final.
[368] FATF, '12-Month Review of The Revised FATF Standards on Virtual Assets And Virtual Asset Service Providers' (FATF, 2020) <www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html> accessed 06 November 2020.
[369] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and amending Directive (EU) 2019/1937 COM(2020) 593 final Title I Art. 1.
[370] Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology COM(2020) 594 final Art. 1.
[371] ibid.
[372] ibid., Art. 9.

and firms themselves gain valuable knowledge about the application of DLT'.[373] The regulation has a five-year review period to ascertain issues that arise in this nascent area.[374] While this proposed regulation makes significant improvements to the financial DLT regulatory landscape, there is still much to be done to foster a strong relationship between decentralised financial technologies and security regulation.

The Likelihood of Blockchain's Continued Relevance to the Financial Sector

In certain respects, decentralised financial technologies like blockchain appear peripheral to a discussion of financial cybersecurity in the EU. Blockchain's presence in the financial sector is still relatively small and there has been talk of 'blockchain fatigue'.[375] There are also fears that in so far as regulations like the proposed regulation on Markets in Crypto-Assets make it difficult for decentralised financial technologies to operate within the EU, these platforms will therefore choose not to operate at all in the EU.[376] For example, decentralised financial technologies may find it difficult to comply with the following governance requirement:

> Issuers of asset-referenced tokens shall have robust governance arrangements, including a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks to which it is or might be exposed, and adequate internal control mechanisms, including sound administrative and accounting procedures.[377]

As discussed further in Sub-Sections III.V.ii. and iii., the difficulty has to do with the challenge of identifying hierarchies of responsibility on decentralised technologies. However, these concerns do not necessarily mean that financial blockchains' days in the EU are numbered.

With respect to the former concern, 'blockchain fatigue' is primarily a product of trying to fit solutions in a wide variety of sectors to the technology rather than recognising blockchain as the best option for a given solution. As companies use blockchain for its core characteristics (like

[373] Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology COM(2020) 594 final 4.
[374] ibid., Art. 10.
[375] Jemima Kelly, 'Blockchain: Disillusionment Descends on Financial Services' (*Financial Times*, 24 September, 2019) <https://www.ft.com/content/93140eac-9cbb-11e9-9c06-a4640c9feebb> accessed 06 October 2020; 'Gartner Predicts 90% of Blockchain-Based Supply Chain Initiatives Will Suffer 'Blockchain Fatigue' by 2023' (Gartner, 7 May 2019) <https://www.gartner.com/en/newsroom/press-releases/2019-05-07-gartner-predicts-90--of-blockchain-based-supply-chain> accessed 06 October 2020.
[376] Werner Vermaak, 'MiCA: A Guide to the EU's Proposed Markets in Crypto-Assets Regulation' (*Sygna*) <www.sygna.io/blog/what-is-mica-markets-in-crypto-assets-eu-regulation-guide/> accessed 27 December 2020.
[377] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and amending Directive (EU) 2019/1937 COM(2020) 593 final Art. 30.

tamper-evident public record keeping and distributed consensus mechanisms) more strategically, blockchain has the potential to persist in relevant sectors.[378] Blockchain has been, and will likely continue to be, of use to the financial sector.[379]

With respect to the latter concern, regulations like the proposed one on Markets for Crypto-Assets can potentially be made more palatable and effective where consortium(s) of decentralised financial technologies liaise with regulators and competent authorities while developing appropriate security mechanisms out of their own initiative. Section IV.V. puts forward suggestions with respect to just such an EU-level consortium.

This section considers the extent to which blockchains are cybersecure, what the incident reporting process is, and blockchain's uncomfortable relationship with some relevant regulations.

i. Cyber Incidents on Blockchains

As much as distributed ledger technologies are lauded for their security aspects, such as immutable record keeping and distributed consensus[380], significant cyber incidents have occurred on the platforms (see Appendix v. and vi. for Ethereum Hack and 51% attack discussion).[381] A table of the types of cyber incidents that can occur on blockchain is found in Appendix vii.. A particularly notable incident was the collapse of the Japanese Mt Gox exchange which resulted in the loss of €460 million in 2011 (see Appendix iv.). Incidents of magnitude might conceivably destabilise sections of the mainstream financial sector if blockchain becomes more integrated. In light of this, the issues of how to report incidents and how to safely scale blockchain across different jurisdictions with different regulations is, thus, relevant to the financial sector's cybersecurity.

ii. Incident Reporting on Blockchains

Incident reporting for decentralised technologies can be challenging. For one, oversight and incident reporting processes for decentralised tech have been relatively fragmented prior to the

[378] Aaron Hurst, 'Determining and Overcoming Blockchain Fatigue' (Information Age, 21 July 2020) <https://www.information-age.com/determining-overcoming-blockchain-fatigue-123490369/> accessed 06 October 2020; 'Is Blockchain Fatigue really Going to Set in by 2022?' (Asia Blockchain Review, 18 February 2020) <https://www.asiablockchainreview.com/is-blockchain-fatigue-really-going-to-set-in-by-2022/ > accessed 06 October 2020.
[379] Kevin Werbach, *The Blockchain and the New Architecture of Trust* (*MIT Press*, 2018).
[380] Chris Hammerschmidt, 'Consensus in Blockchain Systems. In Short.' (*Medium,* 27 January 207) < https://medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe > accessed 06 October 2020.
[381] Mike Orcutt, 'Once Hailed as Unhackable, Blockchains are Now Getting Hacked' (*MIT Technology Review*, 19 February 2019) < https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/ > accessed 06 October 2020.

Commission's recent proposals.[382] For another, incident reporting for decentralised tech is challenged by the problem of identifying controllers / responsible parties (especially in the EU as per the GDPR).[383] This is a problem because a decentralised system like blockchain is based on the notion that each node has equal stake and responsibility in the network. In the case of decentralised cryptocurrency networks, it is usually unclear which individual or organisation is responsible for a given area of the system's management. When an incident occurs or a vulnerability is detected, it can be challenging to determine who in the system might bear responsibility.[384] Given minimal hierarchy, there can also be confusion about who should report an incident or vulnerability that affects multiple nodes. Offsetting these identification issues would require more effective network management and oversight.

Incident reporting for financial decentralised ledger technologies is addressed in the 24 September 2020 proposal for a regulation on 'a pilot regime for market infrastructures based on distributed ledger technology'.[385] As per Article 9, 'operators of DLT market infrastructures shall notify the said competent authorities and ESMA'. However, although the draft states that '[t]he operators of DLT market infrastructures shall provide the competent authority which granted the specific permission and ESMA with any relevant information they may require'[386], particular contents of such notifications are not specified. In addition, these incident reporting requirements do not detail how to handle issues of identifying responsible parties.

iii. Blockchain's Uncomfortable Relationship with Regulations

Furthermore, cross-jurisdictional regulatory disparities and the disjunction between blockchain and regulation within a given jurisdiction can create vulnerabilities for internationally-scaled financial tools that integrate blockchain.[387] While the 24 September 2020 proposals for a regulation on 'a pilot regime for market infrastructures based on distributed ledger technology' and for a regulation on Markets in Crypto-Assets significantly contribute towards harmonisation, work remains to be done to ensure that industry-level blockchain systems involving financial

[382] Tom Lyons, Ludovic Courcelas, and Ken Timsit, 'Legal and Regulatory Framework of Blockchains and Smart Contracts' (*EBOF,* 2019).
[383] Jean Bacon et al., 'Blockchain Demystified: A Technical And Legal Introduction To Distributed And Centralised Ledgers' (2018) 25 Rich JL & Tech.
[384] ibid.
[385] Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology COM(2020) 594 final.
[386] ibid.
[387] Yanling Chang et al., 'Blockchain in Global Supply Chains and Cross Border Trade: A Critical Synthesis of the State-of-the-Art, Challenges and Opportunities' [2020] 58(7) International Journal of Production Research 2082-2099.

institutions in different jurisdictions can achieve regulatory compliance, particularly with respect to anti-money laundering protections and GDPR requirements. Further harmonising reporting, management, oversight, and standards across multiple jurisdictions would help to reinforce financial cybersecurity.

Blockchain's premises of anonymity, immutable record-keeping, and decentralisation make its compliance with a number of regulations challenging.[388] The Collingridge dilemma helps to understand blockchain's tension with certain data protection and cybersecurity regulations (see Section III.IV.). According to the Collingridge Dilemma, while technology cannot be fully regulated until it matures, it is difficult to intervene in the status quo of an already established and mature technology.[389] Blockchain's proliferation and relationship with cybersecurity is challenged both by blockchain's difficulties in complying with reporting, identification, and accountability frameworks and the difficulties of applying those frameworks to this emerging technology. The remainder of this section's discussion of blockchain thus delves deeper into the difficulties of reporting incidents, handling cyber-crime, and attributing accountability on blockchain platforms in relation to blockchain's disjunction with relevant regulations.

Blockchain challenges Anti-Money Laundering (AML) and GDPR mechanisms for accountability attribution, which, in turn, pose a challenge for blockchain. AML regulation was one of the forerunners in developing relevant identification and accountability principles. The relationship of AML regulation and blockchain highlights a number of security and compliance issues that are common themes for blockchain. After discussing AML, this section turns to blockchain's relationship with GDPR, which has a particularly direct bearing on incident reporting and handling for blockchain. Suggestions for blockchain governance are then put forward in Section IV.V.

[388] Yanling Chang, et al., 'Blockchain in Global Supply Chains and Cross Border Trade: A Critical Synthesis of the State-of-the-Art, Challenges and Opportunities' [2020] 58(7) International Journal of Production Research 2082-2099.
[389] Paolo Tasca and Tomaso Aste, 'Crypto-Assets and the Regulator's Role: Ignore, Regulate or Kill?' (*Open Access Government,* 18 July 2018) <//www.openaccessgovernment.org/crypto-assets-and-the-regulators-role-ignore-regulate-or-kill/47858/ > accessed 08 October 2020.

Privacy and Blockchain: Case Study of AML Regulation

Blockchain's decentralisation and adherence to the anonymity principle make it particularly challenging to implement AML regulation in the domain of public blockchains. Money laundering is a process whereby illegal funds are distributed through numerous financial transactions before routing back to the money launderer. The purpose of doing this is to obfuscate the often-illicit origins of funds. In order to combat money laundering, many businesses follow know your customer (KYC) and suspicious transaction reporting (STR) guidelines so that the flow of money can be traced. Inter-business cooperation and information exchange are other ways of countering money laundering. AML implementation is also important for combating more serious money laundering, like terrorist financing.[390]

The Financial Action Task Force (FATF) is 'an independent inter-governmental body' that has stipulated standards with respect to implementing international AML guidelines, and KYC and STR are among its main goals.[391] Both KYC and STR require some degree of hierarchical intervention. This is necessary for verifying identities and monitoring/reporting the money flow through a financial network. Since most public blockchain networks (such as Bitcoin) are decentralised and guarantee anonymity to the transacting entities, it is challenging to comply with KYC and STR.[392] This challenge makes combating money laundering on blockchains difficult, since anonymous transacting entities can contact a digital/crypto exchange to convert their laundered digital funds into fiat money.

To take a more concerted approach to virtual assets, the FATF established the Travel Rule in 2019.[393] The Travel Rule entails that virtual asset (e.g., cryptocurrency) transfers of a certain magnitude between two transacting parties require Virtual Asset Service Providers (VASPs) to identify the 'originator' and 'beneficiary' of the transfer. This requires having the appropriate network monitoring services in place in order to detect illicit transfers in a timely fashion. While compliance with the Travel Rule remains a challenging prospect for many decentralised financial

[390] 'United Nations Convention Against Transnational Organized Crime and The Protocols Thereto' (*United Nations: Office on Drugs and Crime*, 2004).
[391] Yurika Ishii, 'Blockchain Technology and Anti-Money Laundering Regulations under International Law' (*American Society of International Law*, 22 February 2019) <www.asil.org/insights/volume/23/issue/1/blockchain-technology-and-anti-money-laundering-regulations-under#_edn2> accessed 08 October 2020; 'United Nations Convention Against Transnational Organized Crime and The Protocols Thereto' (*United Nations: Office on Drugs and Crime*, 2004).
[392] 'Virtual Currencies Key Definitions and Potential AML/CFT Risks' (*Financial Action Task Force*, 2014).
[393] FATF, '12-Month Review of The Revised FATF Standards on Virtual Assets And Virtual Asset Service Providers' (FATF, 2020) <www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html> accessed 06 November 2020.

technologies—since the infrastructure for its facilitation is in many cases still a work in progress and requires cooperation between decentralised platforms—it is a challenge that several cryptocurrency platforms are looking to tackle with a proof-of-ownership process as well as with the decentralised OpenVASP protocol that is being launched and further developed in cooperation with VASPs.[394]

While there are techniques to de-anonymise individual clients in public blockchain networks such as Bitcoin[395], these techniques are in large part the result of individual and independent research at present. One potential method could be to make use of a technique similar to Zero-Knowledge Proofs, according to which a client node would be capable of proving its real identity without actually revealing sensitive information to the relevant entity.[396]

In light of the above, there is the need and desire for more standardised and international frameworks for identifying actors on decentralised technologies in a way that conforms to AML regulations and respects the premises of decentralisation and privacy. At the same time, a degree of hierarchical intervention is necessary for carrying out AML, KYC, STR, and incident reporting operations. The 'softly-centralised' governance and oversight consortium suggested in Section IV.V. seeks to balance these various elements.

Issue of Accountability Attribution: Blockchain and GDPR

GDPR is a data-privacy legislation with cybersecurity relevance that presents various identification and accountability mechanisms.[397] Some argue that GDPR was already outdated by the time it came into existence since it did not take into consideration decentralised technologies like blockchain.[398] Others take the position that it is the responsibility of the private sector to be informed about relevant regulations and to shape innovations in compliance with it.[399] Irrespective of which position one takes, it is evident that blockchain has difficulties complying

[394] Stephanie Hanselmann, 'What is the FATF Travel Rule?' (*Bitcoin Suisse*) <www.bitcoinsuisse.com/research/specials/what-is-the-fatf-travel-rule> accessed 16 December 2020; Kristin Broughton, 'Crypto Firms Assess How to Comply with Anti-Money-Laundering Standards' (*The Wall Street Journal*, 16 September 2019) <www.wsj.com/articles/crypto-firms-assess-how-to-comply-with-anti-money-laundering-standards-11568626200> accessed 16 December 2020.
[395] Alex Biryukov et al., 'Deanonymisation of Clients in Bitcoin P2P Network' (*Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014).
[396] Lily Hay Newman, 'Hacker Lexicon: What are Zero-Knowledge Proofs?' (*Wired*, 14 September 2019) <www.wired.com/story/zero-knowledge-proofs/> accessed 30 September 2020.
[397] 'General Data Protection Regulation: GDPR' (*GDPR Info*) <https://gdpr-info.eu/ > accessed 08 October 2020.
[398] Tom Cox and Andrew Solomon, 'Blockchain: Is the GDPR Already Outdated?' (*Tech Law for Everyone*, 5 September 2017) <www.scl.org/articles/9994-blockchain-is-the-gdpr-already-outdated> accessed 08 October 2020.
[399] 'Complete Guide to GDPR Compliance', (*GDPR*, 2020) < https://gdpr.eu/ > accessed 08 October 2020.

with GDPR's requirements for controllers, processors, and erasure, and that those requirements are difficult to apply to decentralised technologies in general.

The tension between GDPR and blockchain in these areas poses particular difficulties for attributing, reporting, and handling blockchain incidents.[400] For example, controller identification is important for accurate incident reporting (see Sub-Section II.ix.). Furthermore, GDPR operates upon the assumption that there is a single or small group of entities that can be held accountable for the security and data of a system. It is increasingly debated whether the decentralised nature of blockchain can adequately fit into this model.

These features make it problematic for blockchain technologies to comply with regulations like the GDPR, which have been in force in the EU since 2016.[401]

Issue of Identifying Controllers: Blockchain and GDPR

The GDPR assumes that there is a controller against whom the data subject can assert their rights and who can be held accountable by the national data protection authorities if there is a breach of these rights.[402] As per GDPR, a *controller* sets out the reasons and methods of data processing, and *processors* process this data accordingly.[403] While there can potentially be ways of distinguishing controllers and processors on some public blockchain platforms like Bitcoin, there remains considerable ambiguity.[404]

On the one hand, there are different Bitcoin actors that could potentially qualify as controllers: the users running lightweight Bitcoin nodes who perform financial transfers, the users running full nodes who also validate the correctness of these transfers, the miners who create new blocks and validate new transactions, and the developers of the Bitcoin protocol. The miners are the nodes that validate the transactions and append new blocks to a blockchain. The users and the miners carry out their respective tasks according to the Bitcoin protocol. While developers determine the protocol's content, it is the user collective and miners who decide what version of the protocol to impose on the network. Therefore, it is debatable whether the controllers are a

[400] Dave Michels, 'Here's How GDPR and the Blockchain Can Coexist' (*The Next Web*, 26 July 2018) <https://thenextweb.com/syndication/2018/07/26/gdpr-blockchain-cryptocurrency/> accessed 08 October 2020.
[401] ibid.
[402] 'General Data Protection Regulation: GDPR' (*GDPR Info*) <https://gdpr-info.eu/> accessed 08 October 2020.
[403] ibid.; 'What is a Data Controller or a Data Processor?' (*The European Commission*) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en> accessed 16 December 2020.
[404] Dave Michels, 'Here's How GDPR and the Blockchain Can Coexist' (The Next Web, 2018) <https://thenextweb.com/syndication/2018/07/26/gdpr-blockchain-cryptocurrency/> accessed 08 October 2020.

collective of users and/or miners (see Article 4(7) of the GDPR) or whether users and/or miners act as joint controllers (see Article 26 of the GDPR). Under the current definition of a controller, any individual who runs the blockchain software (i.e., a node) could be considered a joint controller. Consequently, any one of these individuals could theoretically be held accountable by a data protection authority. However, these individuals have little power to amend or correct a block once it has been appended to the chain. In light of the above, the assumed bitcoin controllers have difficulty determining and fulfilling the GDPR responsibilities of controllers in the blockchain context. Given the question of who counts as a controller, it is often problematic to identify responsible actors if an incident occurs on a blockchain network.

III.VI. INCOMPLETE INSURANCE FOR CYBER WARFARE / TERRORISM

Cyber insurance is an emerging aspect of the insurance market. As with conventional insurance policies, a digital service provider may choose to purchase an insurance policy against loss or damage from cyber threats at the cost of an insurance premium. Cyber insurance covers the liabilities and losses that arise when a business engages in digital activities. Importantly, cyber insurance covers businesses' liability for breaches of data, including customers' personal information. It can be used to cover claims, fines/penalties, and loss resulting from theft.[405] It creates a market-based mechanism for spreading out cybersecurity risks.

Advocates for cybersecurity insurance believe that the pre-requisites for insurance coverage will incentivise buyers to take adequate measures towards strengthening their digital infrastructure, which increases the resilience of the overall cybersecurity landscape.[406] Therefore, it is important to strengthen cyber insurance offerings with the aim of developing a fully-fledged cyber insurance market. For such a market to work effectively, however, the industry itself needs to be cushioned from risks to a greater extent.[407]

Although the cyber insurance market is developing, it is nascent compared to the insurance industry's other areas.[408] The effects of cyber incidents can be difficult to calculate and therefore pose a challenge to classical insurance theory and practice.[409] National governments and the insurance market are making considerable strides to strengthen this element of the financial system's resilience against cyber incidents, but the cyber insurance market remains largely incomplete at present.[410]

Section III.VI. looks first at war and terrorism exclusion clauses, which are important issues in the existing cyber insurance market. Such exclusions in the private sector make the financial system more vulnerable to cyber-induced systemic instability, especially if there are also no special insurance mechanisms in place (e.g., national terrorism risk insurance programmes). The state of national terrorism risk insurance programmes is the second topic this section discusses.

---

[405] 'Cyber and Privacy Insurance' (*IRMI*) <https://www.irmi.com/term/insurance-definitions/cyber-and-privacy-insurance> accessed 1 March 2020.
[406] Rebecca Lucas, James Sullivan, Jason R.C. Nurse, 'Incentivising Cybersecurity through Cyber Insurance' (*Royal United Services Institute*, 2020) <https://rusi.org/projects/incentivising-cybersecurity-through-cyber-insurance> accessed 30 July 2020.
[407] Maria Demertzis and Guntram Wolff, 'Hybrid and Cybersecurity Threats and the European Union's Financial System' (*Bruegel,* 2019) 11; EIOPA, *Cyber Risk for Insurers—Challenges and Opportunities* (2019) 3-4.
[408] EIOPA, *Cyber Risk for Insurers—Challenges and Opportunities* (2019) 3-4.
[409] ibid., 8; OECD, *The Role of Cyber Insurance in Risk Management* (OECD Publishing, 2017) 93-103.
[410] See preceding citation.

Relatively few member states develop such programmes through private-public partnerships, and such programs can differ widely in the extent to which they cover cyber terrorism. This section also highlights that classical insurance time frames may not be rapid enough to forestall loss of market confidence in the event of a large cyber incident on one or more financial institutions.

In light of these issues, Section IV.VI. expands on existing initiatives for insuring against cyber war and cyber terrorism and puts forward suggestions in this area.

i. Cyber War and Cyber Terrorism Exclusion Clauses

Cyber warfare includes offensive measures that seek to degrade, sabotage, or render a country's information technology infrastructure incapable of normal operation.[411] A frequently cited definition focused on nation-state conflict is found in Richard Clarke and Robert Knake's seminal book, *Cyber War*, and reads, 'actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or disruption'.[412] The 2019 Verizon 'Data Breach Investigations Report' indicates that 23% of such breaches are linked to state actors.[413] Such attacks can include distributed denial of service attacks, viral malwares, ransomware, and other forms of cyber extortion.[414]

With cyber incidents like the NotPetya attack—which caused almost $80 billion in damages—there are doubts about the extent to which the cyber insurance industry can withstand the burden of insuring such attacks.[415] As more companies fall victim to attacks from state-backed actors, many insurers take the position that they do not cover such events. Many insurance contracts now include a war exclusion clause.[416] Even in the growing area of the insurance market that

[411] Louis Marinos et al., 'ENISA Threat Landscape Report 2018'(*ENISA*, 2018) 122; Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (Harper Collins, 2010).
[412] Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (Harper Collins, 2010) 6.
[413] Verizon 2019 'Data Breach Investigations Report' [not open access] quoted in Judy Selby and Peter McLaughlin, 'Is Insurance Coverage for Cyber Claims Barred by War Exclusion?' (*20iapp*, 25 June 2019), <https://iapp.org/news/a/setting-the-record-straight-on-cyberinsurance-claim-denials-and-the-war-exclusion/> accessed 3 March 2020.
[414] 'Cyber Warfare' (RAND Corporation, 2020) <www.rand.org/topics/cyber-warfare.html> accessed 14 April 2020.
[415] Nicole Lindsey, 'Insurance Not Valid in Case of Cyber War, Says Major Insurance Company' (*Chief Privacy Officer Magazine*, 17 January 2019) <www.cpomagazine.com/cyber-security/cyber-insurance-not-valid-in-case-of-cyber-war-says-major-insurance-company/> accessed 6 March 2020; Alistair Gray, 'Cyber Risks Too Big to Cover, Says Lloyd's Insurer: Governments Should Step in to Provide Aid, Says Catlin Boss' (*Financial Times*, 5 February 2015) <https://www.ft.com/content/94243f5a-ad38-11e4-bfcf-00144feab7de> accessed 20 September 2020; Cyber Risks – Insurable, But Within Limits' (*Swiss Re*) <www.swissre.com/reinsurance/property-and-casualty/solutions/cyber-solutions/cyber-risks-insurable-but-within-limits.html> accessed 23 September 2020.
[416] Patrick Bracher, 'Cyber Insurance and the War Exclusion | Financial Institutions Legal Snapshot' (*Norton Rose Fulbright: Financial Institutions Legal Snapshot*, 16 July 2019). <www.financialinstitutionslegalsnapshot.com/2019/07/cyber-insurance-and-the-war-exclusion/> accessed 6 March 2020.

explicitly seeks to cover warfare (and/or terrorism), some incident variants are sometimes excluded.[417] Exclusion clauses and an absence of alternative insurance mechanisms compound the difficulty of companies' positions, given that cyber warfare has the potential to leave even the largest organisations reeling.[418]

The ongoing dispute since 2018 between Mondelez International (one of the companies most affected by the NotPetya attack) and Zurich American Insurance Co., indicates current uncertainty about when a cyber incident can be considered warfare or (as in Zurich's policy) 'a hostile or warlike action'. In this case, the dispute centers less on whether it was state-backed or not (several governments' intelligence points to the Russian military), but rather whether it qualifies as 'hostile or warlike'.[419] Zurich's decision to argue that it does not cover the NotPetya repercussions because it was a state-backed hostility stands in juxtaposition to the insurance Marriot received for a similar degree of losses (over $100 million) from a cyberattack allegedly linked to the Chinese government.[420]

Even where an incident is deemed 'hostile or warlike', the question of whether it was state-backed and what counts as state-backing may need to be clarified. Cyber terrorism tends not to be excluded by war exclusion clauses, but this is an ambiguous area.[421] To reduce such ambiguity, some insurance companies have clauses that specifically exclude cyber terrorism.[422]

---

[417] Felton Johnston, 'Cyberwar/Cyberterrorism—A Challenge for Insurers and Cross-Border Investors' (*Robert Wray PLLC*, 28 May 2019) <www.robertwraypllc.com/cyberwar-cyberterrorism-a-challenge-for-insurers-and-cross-border-investors/> accessed 25 September 2020.

[418] Nicole Lindsey, 'Cyber Insurance Not Valid in Case of Cyber War, Says Major Insurance Company' (*Chief Privacy Officer Magazine*, 17 January 2019) <www.cpomagazine.com/cyber-security/cyber-insurance-not-valid-in-case-of-cyber-war-says-major-insurance-company/> accessed 6 March 2020.

[419] 'NotPetya' (*CFR*, July 2017) <www.cfr.org/cyber-operations/notpetya> accessed 20 September 2020; 'Statement from the Press Secretary' (*The White House*, 15 February 2018) <www.whitehouse.gov/briefings-statements/statement-press-secretary-25/> accessed 20 September 2020; 'Russian Military 'Almost Certainly' Responsible for Destructive 2017 Cyber-Attack' (*NCSC UK*, 14 February 2018) <www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack> accessed 20 September 2020; Felton Johnston, 'Cyberwar/Cyberterrorism' (*Robert Wray PLLC*, 28 May 2019) <www.robertwraypllc.com/cyberwar-cyberterrorism-a-challenge-for-insurers-and-cross-border-investors/> accessed 25 September 2020.

[420] Andrew Parsons, Katie Simmonds, Jenny Gibbs, 'A Cyber-Attack vs An Act of Aar: Conflicting Positions in Marriott and Mondelez' (*Womble Bond Dickinson (UK) LLP* and *Lexology*, 31 January 2020) <www.lexology.com/library/detail.aspx?g=dec0f622-5ee6-4de9-8ff2-d6b9e4adaf8c> accessed 22 September 2020.

[421] Mirza Salam Ahmed and Ben Dyson, 'Cyber Insurance Wrestle with War Exclusions as State-Sponsored Attack Fears Grow' (*S&P Global Market Intelligence*, 30 January 2020) <www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyber-insurers-wrestle-with-war-exclusions-as-state-sponsored-attack-fears-grow-56743302> accessed 25 September 2020.

[422] Felton Johnston, 'Cyberwar/Cyberterrorism—A Challenge for Insurers and Cross-Border Investors' (*Robert Wray PLLC*, 28 May 2019) <www.robertwraypllc.com/cyberwar-cyberterrorism-a-challenge-for-insurers-and-cross-border-investors/> accessed 25 September 2020; Simon Shooter, 'Cyber Insurance: Debunking the Myths' (*Bird & Bird LLP* and *Lexicology*, 28 June 2019) <www.lexology.com/library/detail.aspx?g=26cddd55-b7ab-495d-b832-afc4a37fcac1> accessed 24 September 2020.

It is difficult to know how to effectively regulate the situation until pending landmark cases like *Mondelez vs. Zurich* have been decided by the courts. The pace of regulation is also affected by the widespread recognition that the insurance market is still in the early stages of developing the tools and expertise required to provide policies appropriate to the current cybersecurity landscape.[423] Until a decision is made on pending cases and the insurance market develops further, regulators will find it difficult to regulate the insurance market on this matter. Instead, governments can set up their own initiatives, potentially in cooperation with the private sector.

ii. Few National Terrorism Risk Insurance Programmes

Some in the insurance industry have been engaging with governments to re-evaluate war and/or terrorism exclusion clauses.[424] Aspects of the US insurance market as well as the terrorism risk insurance programme, run by Pool Re in collaboration with the UK government, have taken steps in this direction.[425] Lloyd's bank in the UK has also considered the topic.[426]

The OECD conducted a study on terrorism risk insurance in its member countries in 2016.[427] Most OECD member states do not have national terrorism risk insurance programmes established by, or acting in conjunction with, the government. Rather, many leave it wholly to the insurance market to develop any national-level initiatives.[428] As of 2016, national programmes associated with respective governments were only present in ten OECD countries. EU (or formerly EU) countries with government-associated national programmes include Belgium, Denmark, France, Germany, the Netherlands, Spain, and the UK. Austria has a national programme, but it is a private-sector one.[429]

The extent to which cyber incidents are covered by the programmes of these EU member states varies significantly. Spain and France explicitly cover certain aspects of cyber incidents. Spain's

[423] HM Government Department for Digital, Culture, Media, and Sport, 'Cyber Security Regulation and Incentives Review' (2016) 3.
[424] OECD, 'Cyber Insurance Market Challenges' in *Enhancing the Role of Cyber Insurance in Risk Management* (2017) 101.
[425] ibid.; Carolyn Cohn, 'Terrorism Reinsurance Fund in UK Wants to Add Cyber Cover' (*Carrier Management*, 10 March 2017) <www.carriermanagement.com/news/2017/03/10/165134.htm> accessed 19 September 2020; Sonali Basak, 'Worried About a Cyber-Apocalypse? AIG Wants to Sell You a Policy' (*Bloomberg*, 22 July 2015), <www.bloomberg.com/news/articles/2015-07-22/worried- about-a-cyber-apocalypse-aig-wants-to-sell-you-a-policy> accessed 19 September 2020.
[426] 'Facing the Cyber Risk Challenge: A Report by Lloyd's (*Lloyd's*, 2016); OECD, 'Cyber Insurance Market Challenges' in *Enhancing the Role of Cyber Insurance in Risk Management* (2017) 101.
[427] OECD, 'National Terrorism Risk Insurance Programmes of OECD Countries with Government Participation' (2016).
[428] ibid.
[429] 'Terrorism Risk Insurance Programmes by Country' (*OECD*) <www.oecd.org/daf/fin/insurance/terrorism-risk-insurance-programmes.htm> accessed 30 March 2020.

programme 'likely' covers physical damage and bodily injury due to cyber-attacks. It 'potentially' covers data and software loss.[430] France's programme 'likely' covers physical damage. Cyber incidents are unambiguously not covered by the German and UK programmes as of the writing of the OECD report. As indicated above, there have subsequently been some steps in the UK towards changing this.[431] However, most national terrorism risk programmes in the EU, in so far as they exist, are hands off about cyber incident coverage.

[430] OECD, 'Cyber Insurance Market Challenges' in *Enhancing the Role of Cyber Insurance in Risk Management* (2017) 100.
[431] ibid., 101.

III.VII. (CYBER-INDUCED) SYSTEMIC RISK AND BANK RESOLUTION

In light of the upheavals of the 2008-2012 Global Financial Crisis and the growing recognition of cyber-induced systemic risk, this section looks at the relationship of cybersecurity, systemic risk, and the Eurozone's banking union, paying particular attention to cyber-induced systemic risk and the incompleteness of that banking union.

These issues are followed-up in Section IV.VII., which discusses methods that can contribute to maintaining market confidence in the event of a large cyber incident against the financial system. Special attention is given to the role public funding could play once private sector insurance options are exhausted, particularly in the context of cyber-induced systemic risk.

i. Background on Systemic Risk and the Fragility of a Monetary-Only Union

Financial systemic risk is the risk that the financial system will be destabilised by an incident at the company level and vice versa. In some cases, loss of confidence in even just a few financial institutions can trigger systemic instability across the entire financial sector if these institutions are large and/or deeply enmeshed in the system. The following outline of the 2008-2012 Global Financial Crisis provides background on systemic financial instability induced by non-cyber factors. The European experience of the Global Financial Crisis arose from a confluence of many factors that illustrate how a loss of market confidence can generate systemic instability. A significant element in the Eurozone's case was the fragility of a monetary union that was not systematically complemented by a banking union.

US Subprime Mortgage Crisis

Among other issues, loan market deregulation (in the US housing market especially), system opacity, and overconfidence in existing economic models exacerbated systemic risk in the lead-up to the 2008-2012 crisis.[432] Subprime loans became commonplace during the US housing bubble. Financial instruments that incorporated these loans were in increasing demand. These instruments were considered low-risk because they were not the only component of the financial instruments, and there was thought to be enough diversification in banks' portfolios.[433] When demand for houses began to slow and house prices dropped, the interest on many of those

[432] Alan Taylor, *Credit, Financial Stability, and the Macroeconomy* (National Bureau of Economic Research, 2015) 1; Mervyn King, *The End of Alchemy: Money, Banking, and the Future of the Global Economy* (W. W. Norton & Company, 2017) 26-27, 35-36; Mark Blyth, *Austerity: The History of a Dangerous Idea* (Oxford University Press, 2013) 21-50.
[433] Mervyn King, *The End of Alchemy: Money, Banking, and the Future of the Global Economy* (W. W. Norton & Company, 2017) 104.

subprime loans increased.[434] Borrowers who could not afford the new interest rates defaulted, and many lenders went bankrupt.[435] Because the secondary market for subprime loans was a global one, the crisis became international.[436]

As confidence in these financial instruments dropped, there was a rush to sell. In addition, it became difficult to tell which banks had invested in affected instruments. Lending between banks slowed to a trickle, and liquidity was increasingly difficult to obtain.[437] Many banks also did not have enough capital to sufficiently mitigate their exposure to the loans they had made.[438] Loan maturities became increasingly shorter, such that loans to several European banks suddenly had to be repaid more quickly than expected.[439] There was an increasing recognition that banks throughout the world, but especially in the US and Europe, had much too little capital to justify the loans they had been making. It was thus both a liquidity and a capital crisis.

While not the only reason for the European experience of the Financial Crisis, the subprime mortgage crisis originating in the US was a significant catalyst for the decline in market confidence. Once investors began to lose confidence in the financial markets, the contagion spread quickly. Many banks failed as part of a chain reaction across highly integrated financial networks.

The European Sovereign Debt Crisis

The widespread loss of market confidence in the Eurozone was a confluence of this subprime mortgage crisis, some EU countries' own housing bubbles, cases of low growth, and the conditions of the monetary union. Because banking in the EU was more nation-focused at the time, confidence in a member state's banking system was tied to that sovereign's perceived ability to bail out banks and to make good on their own bonds.[440]

A number of factors undermined that confidence. Private sector debt in Ireland and Spain skyrocketed during their respective housing bubbles.[441] Ireland's was particularly entwined with the US' subprime mortgage crisis. Low growth and demographic issues in Italy and Portugal

[434] Will Kenton, 'Financial Crisis' (*Investopedia,* 16 March 2020) <www.investopedia.com/terms/f/financial-crisis.asp> accessed 1 November 2020.
[435] ibid.
[436] ibid.
[437] Mervyn King, *The End of Alchemy: Money, Banking, and the Future of the Global Economy* (W. W. Norton & Company, 2017) 36.
[438] ibid.
[439] ibid., 37.
[440] Nicholas Véron, *Europe's Radical Banking Union* (Bruegel, 2015) 14.
[441] Mark Blyth, *Austerity: The History of a Dangerous Idea* (Oxford University Press, 2013) 64-68.

undermined confidence in the sovereigns' ability to make good on their debt, although the amount of that debt was not outrageous in comparison to other EU member states.[442] A decrease in Greece's economic competitiveness, its ineffective tax collection, and its fragmented approach to public spending resulted in a debt crisis.[443] In all these countries, private and public sector lending and spending increased with their adoption of the Euro, since they were perceived as being under the same credit rating as Germany on the basis that the European Central Bank (ECB) could theoretically act as the lender of last resort, even if it had no express mandate to do so.[444] European banks thus significantly invested in these countries' government bonds, generating a close relationship between the banking system and sovereign debt.

Eventually, the housing bubbles burst, the unsustainable growth trajectories became obvious, and the problems in Greece's approach to public finance were exposed. As the contagion of lost confidence spread, governments did not have the resources to back up their bonds or offset the banking system's massive exposures. Because monetary policy in the EU lies with the ECB, member states' central banks did not have the power to devalue their currencies in an attempt to mitigate the situation.[445] Whereas countries outside a monetary union can allow their exchange rates to absorb some of the effect of investors selling government bonds of that country in order to buy those of another, that is not an option for individual countries in a monetary union. Consequently, member states could not stoke demand and competitiveness by allowing the currency to depreciate on the exchange rate market.[446] Because the Eurozone had not complemented a monetary union with a banking union, the effects of systemic instability were also not appropriately offset by a common deposit insurance or resolution mechanism.

In order to restore market confidence in the EU, the ECB effectively promised that they would act as a lender of last resort.[447] This promise was beyond the ECB's mandate and was consequently controversial. It did restore confidence, however. The run on banks and the rapid selling of bonds slowed. As discussed further in Sub-Section III.VII.iv., the development of a full banking union has been a hot topic since the crisis, and more elements of such a union have been put in place. The suggestion put forward in Section IV.VII.ii. discusses appropriate

[442] Mark Blyth, *Austerity: The History of a Dangerous Idea* (Oxford University Press, 2013) 68-71.
[443] ibid., 62-64.
[444] ibid., 62, 68, 69.
[445] ibid., 16.
[446] Paul de Grauwe, *Economics of Monetary Union* (Oxford University Press, 2018)
[447] 'Speech by Mario Draghi, President of the European Central Bank at the Global Investment Conference in London 26 July 2012' (*European Central Bank*, 26 July 2012) <www.ecb.europa.eu/press/key/date/2012/html/sp120726.en.html> accessed 19 September 2020.

adjustments to aspects of the (currently incomplete) banking union that would help to mitigate cyber-induced systemic instability.

ii. The Growing Recognition of Cyber-Induced Systemic Risk

After some debate about whether cyber attackers have the capacity to induce systemic instability, cyber-induced systemic risk is increasingly being treated as an important issue by the EU banking system.[448] The European Systemic Risk Board's (ESRB) February 2020 report on the subject recognises the possibility that systemic instability might arise.[449] They base their analysis on data collected by the European Systemic Cyber Group.[450] Although past cyberattacks have not been able to generate a contagion of lost confidence in the financial system, they demonstrate attackers' increasing ability to strike effectively and rapidly across integrated networks.[451] The ESRB's February report recognises that a liquidity crisis and a corresponding loss of market confidence could occur if a cyber incident of scale impacts monetary values held in the financial system.[452] Since market confidence will broadly determine whether a cyber incident becomes a systemic risk, the ESRB's report emphasises the need for more effective information sharing mechanisms between private stakeholders, governments, and the public.[453] It also emphasises the need for clear jurisdictions for dealing with the many facets of such a crisis.[454] As is also indicated by their subsequent research, the ESRB is paying increasing attention to cyber-induced systemic risk.[455]

iii. The Need to Rapidly Allocate Resources to Mitigate Contagion

One method of mitigating cyber-induced systemic risk is to have provisions in place for rapidly allocating funds to stabilise infrastructure and market confidence.[456] As discussed in Section III.VI., there is a general dearth of emergency insurance for cyber incidents of a warlike or terrorist nature. At present, there also does not yet exist emergency funding for cyber incidents at the EU-level. There is no equivalent to the Solidarity Fund, which handles natural disasters, for cyber-disasters. A growing amount of the policy literature on cyber risk is paying attention to

[448] European Systemic Risk Board, *Systemic Cyber Risk* (2020) 52-53.
[449] ibid.
[450] ibid.
[451] ibid., 2.
[452] ibid., 3.
[453] ibid.
[454] ibid.
[455] Greg Ros, 'The Making of a Cyber Crash: A Conceptual Model For Systemic Risk in the Financial Sector' (ESRB, 2020).
[456] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 35-37.

this area. Section IV.VII. analyses existing proposals for emergency funding and puts forward further suggestions on this matter.

iv. Incomplete Banking Union

The issue of how to pre-empt, handle, and mitigate systemic risk in the Eurozone is tied to the debate about whether to create a full banking union. To supporters of a banking union, the Global Financial Crisis and cyber-induced systemic risk serve as compelling arguments in favour of such a project.[457] A full banking union would have the legitimate capacity to ensure deposits, act as a liquidity backstop, resolve/restructure failing banks, and supervise banks' preparedness and prudential standards.[458] The banking union would exercise these competencies at the EU rather than the national level.[459] It would thereby mitigate the fragmentation that exacerbated the EU's experience of the Global Financial Crisis.

Currently, a number of components of such a banking union exist. The European Banking Authority (EBA) and the European Commission serve as regulators. The ECB's supervisory and resolution arms—the Single Supervisory Mechanism (SSM) and the Single Resolution Mechanism (SRM)—supervise bank stability, (de)license banks, run stress-tests, and resolve banks where appropriate.[460] The ECB's controversial promise to act as a lender of last resort is also a component of the partially-formed banking union.[461]

These components were developed in response to the Global Financial Crisis in order to deal more concertedly with its consequences, which were fed and exacerbated by the nation-focused banking that prevailed before and during the Crisis.[462] Although the ECB's promise to act as a lender of last resort mitigates a future run on banks of the scale experienced during the Global Financial Crisis, the issue of how to resolve insolvent banks (such that their collapse does not result in systemic instability) continues to pose a challenge.[463] The EU's semi-complete banking

[457] Nicholas Véron, *Europe's Radical Banking Union* (Bruegel, 2015) 5-6.
[458] 'What is the Banking Union?', (*European Commission*) <https://ec.europa.eu/info/business-economy-euro/banking-and-finance/banking-union/what-banking-union_en> accessed 20 April 2020.
[459] Nicholas Véron, *Europe's Radical Banking Union* (Bruegel, 2015) 9.
[460] ibid., 10.
[461] Daniel Gros and Dirk Schoenmaker, 'European Deposit Insurance and Resolution in the Banking Union' [2014] JCMS, 52(3) 534.
[462] Nicholas Véron, *Europe's Radical Banking Union* (Bruegel, 2015) 20-21.
[463] Daniel Gros and Dirk Schoenmaker, 'European Deposit Insurance and Resolution in the Banking Union' [2014] JCMS, 52(3) 534.

union's missing components include deposit insurance, a full resolution framework, and a fiscal backstop.[464] The banking union remains a politically-difficult work in progress.[465]

v. Question of Funding Bank Resolution Caused by Cyber War/Terrorism

One question worth asking is whether public funding is warranted in cases where banks need to be resolved because an act of cyber war or cyber terrorism causes systemic instability. In recent years the EU has taken significant strides to shift its emphasis from a bail-out to a bail-in (private-only financing) approach, so that financial institutions are accountable for their actions. The EU has not had to face bank resolution caused by cyber warfare/terrorism and therefore has yet to have cause to consider the relationship of such resolution with principles of national security as they pertain to warfare/terrorism. The following provides further background for the suggestion in Sub-section IV.VII.ii. for financing bank resolution in the context of cyber warfare/terrorism.

Existing Deposit Insurance and Bank Resolution Frameworks and Proposals

Spurred by the Global Financial Crisis, the Single Resolution Fund (SRF) pools financial firms' contributions for bank resolution. The SRF provides liquidity to restructure banks that are no longer solvent and the collapse of which poses a systemic risk across the financial system.[466] The SRF places an emphasis on bail-in, which is appropriate for systemic instability induced by human behaviour in the private sector (as was the case in the Global Financial Crisis).

Some policy researchers have proposed merging this bank resolution mechanism with a deposit insurance fund under a European deposit insurance and resolution authority (EDIRA), with the European Stability Mechanism (ESM) acting as a fiscal backstop.[467] Doing so would consolidate the banking union. At present, only the SRF is established, and the European Deposit Insurance Fund is planned as a separate entity.[468] Policy researchers who promote a combined authority (as done in the United States) note that the two functions are enmeshed, with resolution in many

[464] Daniel Gros and Dirk Schoenmaker, 'European Deposit Insurance and Resolution in the Banking Union' [2014] JCMS, 52(3) 534; Nicholas Véron, *Europe's Radical Banking Union* (Bruegel, 2015) 22.
[465] Nicholas Véron, *Europe's Radical Banking Union* (Bruegel, 2015) 7-13.
[466] 'What is the Single Resolution Fund?' (*Single Resolution Board*) <https://srb.europa.eu/en/content/single-resolution-fund> accessed 27 March 2020.
[467] Daniel Gros and Dirk Schoenmaker, 'European Deposit Insurance and Resolution in the Banking Union' [2014] JCMS, 52(3) 530, 537.
[468] ibid 537; 'European Deposit Insurance Scheme: A Proposed Scheme to Protect Retail Deposits in the Banking Union' (*European Commission*) <https://ec.europa.eu/info/business-economy-euro/banking-and-finance/banking-union/european-deposit-insurance-scheme_en#overview> accessed 21 September 2020.

cases effectively acting as deposit insurance.[469] They argue that establishing distinct institutions will likely result in disputes between the two.[470]

The implementation of a deposit insurance authority to complement the SRF (whether combined or separate) as well as an expansion of the ESM into a fiscal backstop would help to complete the banking union.[471]

The Issue of Inadequate Resolution Funding

There are concerns that the SRF is not large enough to deal with some financial crises.[472] As of 17 July 2019, the SRF has €33 billion.[473] If the SRF runs out of funds, the ESM steps in on the condition that the SRF pay it back.[474] There are doubts, however, that even the ESM provides enough of a fallback.[475]

Should governments contribute more to bank resolution? In non-cyber financial crises, it is clear that banks should be bailed-in as much as possible and thus be accountable for their behaviour. The issue is more ambiguous regarding the possibility of bank resolution in response to cyber warfare or cyber terrorism, however.

At present, the ESM is not a direct fiscal backstop. Rather, it is financed through capital market instruments and money market transactions.[476] The ESM provides indirect fiscal backing in so far as Eurozone countries guarantee its financial instruments, which are low-risk.[477]

---

[469] Daniel Gros and Dirk Schoenmaker, 'European Deposit Insurance and Resolution in the Banking Union' [2014] JCMS, 52(3) 537; Merwan H. Engineer, Paul Schure, and Mark Gillis, 'A Positive Analysis of Deposit Insurance Provision: Regulatory Competition among European Union Countries' [2013] JFS 9(4) 530–44; Franklin Allen et al., *Cross-Border Banking in Europe: Implications for Financial Stability and Macroeconomic Policies* (Centre for Economic Policy Research, 2011).
[470] Daniel Gros and Dirk Schoenmaker, 'European Deposit Insurance and Resolution in the Banking Union' [2014] JCMS, 52(3) 537.
[471] ibid.
[472] Willem Pieter de Groen, 'Financing Bank Resolution: An Alternative Solution for Arranging the Liquidity Required—Banking Union Scrutiny' (*Economic Governance Support Unit: Directorate-General for Internal Policies of the Union*, 2018) 4-9, 11, 16-17.
[473] 'What is the Single Resolution Fund?' (*Single Resolution Board*) <https://srb.europa.eu/en/content/single-resolution-fund> accessed 23 September 2020.
[474] Rebecca Christie, *Safeguarding the Euro in Times of Crisis: The inside story of the ESM* (European Stability Mechanism, 2019) 360; European Stability Mechanism, 'What is the Common Backstop?' (2020) <www.esm.europa.eu/content/what-common-backstop-0> accessed 8 December 2020.
[475] Willem Pieter de Groen, 'Financing Bank Resolution: An Alternative Solution for Arranging the Liquidity Required—Banking Union Scrutiny' (*Economic Governance Support Unit*, 2018) 4-9, 11, 16-17.
[476] 'About Us' (*European Stability Mechanism*) <https://www.esm.europa.eu/about-us/intro> accessed 1 August 2020.
[477] Rebecca Christie, *Safeguarding the Euro in Times of Crisis: The Inside Story of the ESM* (European Stability Mechanism, 2019) 87; European Stability Mechanism, 'How We Work' <www.esm.europa.eu/about-us/how-we-work#overview> accessed 8 December 2020.

One option outlined in greater detail in Sub-section IV.VII.ii. would be to add a more direct layer of fiscal backing, in which governments contribute funds to the ESM earmarked for cases of cyber warfare and cyber terrorism that can be used once the initial layer of ESM financial support is used.

IV. SUGGESTIONS

The following sections put forward suggestions for the policy issues presented above. These suggestions engage with and build upon existing policy research in these areas, also taking into account several recent draft regulations and Commission communications that seek to improve financial cybersecurity in the Eurozone and wider EU. The following suggestions aim to complement the highly integrated nature of the EU financial system and the Single Market with a greater degree of harmonised incident mitigation and response than has been implemented as of the writing of this report. At the same time, they aim to leave room for appropriate adaptation to national, regional and sectoral circumstances, albeit whilst reducing existing degrees of fragmentation. In short, the suggestions promote greater harmonisation without seeking to impose homogenisation. This paper's suggestions are intended to serve as points of reference for policy makers and researchers, while also being of potential interest to the general public.

IV.I. INCIDENT REPORTING AND INFORMATION SHARING

In light of the cross-border nature of cyber incidents and the extent to which incident reporting in the EU remains diverse as of the writing of this report, there is a case to be made for further *streamlining incident reporting channels* and *harmonising reporting templates,* which will reinforce information sharing and incident analysis in turn.[478]

Building on cyber hub proposals put forward by a 2018 CEPS-ECRI Task Force and a 2019 European Banking Federation (EBF) report,[479] and taking recent regulatory proposals into account, this paper puts forward suggestions for further centralising reporting frameworks with an eye to mitigating cyber-induced systemic risk and other cross-border implications. The suggested cyber reporting hub could work closely (or even integrate) with EU-CyCLONe, the Cyber Shield, Information Sharing and Analysis Centres (ISACs), and the European vulnerability repository to form a broader incident and vulnerability reporting, analysis, and advisory hub at the EU-level. Such collaboration could proactively bring various participants of the forthcoming Joint Cyber Unit into closer relation. Given practical considerations at this time, one possibility is to direct efforts towards a cyber reporting hub that is specific to the EU's financial sector and is composed of only those financial institutions that the ECB identifies as significant enough to affect the security of other states if a cyber incident of magnitude occurs. This paper also considers adjustments to existing reporting templates.

The suggestions put forward in this section promote greater harmonisation and even a degree of greater centralisation. However, this need not entail wholly homogenised incident reporting across the EU. Rather, the aim is to harmonise to a greater degree in critical areas: in some respects through greater centralisation, in others through more harmonious horizontal relationships. This paper's suggestions for incident reporting thus try to strike a balance between the need for greater coherence and the practical and political arguments for limiting centralisation. On the one hand, there is a need for better cross-border reporting, information sharing, and handling with respect to cross-border incidents against the financial sector. It is widely appreciated that matters of member state (cyber)security are increasingly becoming matters of Union (cyber)security.[480] On the other hand, member states have the duty and

[478] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 2, 14, 18-19.
[479] ibid.; European Banking Federation, 'EBF Position Paper on Cyber Incident Reporting' (2019).
[480] Commission Staff Working Document Impact Assessment accompanying the document Proposal For a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity

prerogative to guard information on matters of national security in sensitive situations. In addition, there is the principle that authorities should pursue methods that work well within local, regional, and sectoral contexts. A cyber hub would need to balance the many considerations pertinent to each side.

i. Existing and Previously Proposed EU Frameworks

The following discussion considers frameworks that currently facilitate, or propose to facilitate, better incident reporting and cross-border information sharing. Cross-border information sharing is particularly expected to see expansive improvement with the implementation of EU-CyCLONe, the JCU, and the European Cyber Shield (see Sub-sections II.x., II.xix., and II.xx. respectively).

Information Sharing and Analysis Centres

ISACs are one of the primary frameworks for information sharing in the EU. The 2018 CEPS-ECRI Task Force highlights ISACs for their two-way information flow capabilities.

There is an international, US-based ISAC for the financial sector (FS-ISAC). However, as of the 2018 CEPS-ECRI report, the FS-ISAC does not adequately incorporate regulators and supervisors in its framework.[481] In addition, the European Cyber Security Organisation (ECSO) position paper on ISACs notes that FS-ISAC's 'European based steering group and threat intelligence committee has insufficient trust-fostering capacity and that the EU's financial security priorities differ from the US'.[482]

In contrast to FS-ISAC, FI-ISAC, the EU's own ISAC for the financial system established in 2008, is a private-public partnership that facilitates information flows between banks, CSIRTs, and law enforcement agencies.[483] However, ECSO indicates that as much as FI-ISAC is an important information sharing platform, it does not amount to a pan-European financial ISAC.[484] ECSO recommends that an information sharing hub should allow the financial institutions to

certification ("Cybersecurity Act") SWD/2017/500 12-14; Cybersecurity Technology and Capacity Building Unit, 'The Cybersecurity Act' (*European Commission* 28 February 2020) <https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act> accessed 10 September 2020; Joint Communication to the European Parliament and the Council The EU's Cybersecurity Strategy for the Digital Decade [2020] JOIN 18 final 3-4.

[481] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 17; 'Become a Member' (*FS-ISAC*) <www.fsisac.com/membership> accessed 1 November 2020.

[482] 'ECSO Position Paper on sector-specific ISACs' (*ECSO,* 2018) 11.

[483] 'European Financial Institutes – Information Sharing and Analysis Centre, A Public-Private Partnership' (*ENISA*).

[484] 'ECSO Position Paper on sector-specific ISACs' (*ECSO,* 2018) 11-12.

have a greater say in its governance and operations.[485] ECSO further argues that a hypothetical pan-European financial ISAC should be a flexible hub that guides and connects information mechanisms appropriate to local and sectoral circumstances.[486]

The European Cyber Shield

As per the new EU Cybersecurity Strategy, the European Cyber Shield will be a strengthened and expanded 'network of Security Operations Centres across the EU'.[487] The participating SOCs will perform an analysis and information sharing role, specifically,

> ...to more efficiently share and correlate the signals detected and create high-quality threat intelligence to be shared with ISACs and national authorities, and thus enabling a fuller situational awareness...to create collective knowledge and share best practices...to improve incident detection, analysis and response speeds through state-of-the-art AI and machine learning capabilities...this network will provide timely warnings on cybersecurity incidents to authorities and all interested stakeholders, including the Joint Cyber Unit. [488]

The Joint Cyber Unit

Similarly, the JCU places an emphasis on developing a '"need-to-share" mind-set' across the EU (see Section II.xix.).[489] The JCU would consist of closer cooperation between existing institutions in accordance with their existing 'competences and powers', rather than being instantiated as an entity.[490] Instead of being 'an additional, stand-alone body', it would 'act as a backstop where the participants can draw on one another's support and expertise, especially in the event that various cyber communities are required to work closely together.'[491] It would offer 'a virtual and physical platform for cooperation for the different cybersecurity communities in the EU, with a focus on operational and technical coordination against major cross border cyber incidents and threats.'[492]

The JCU's aims include the following:

> Firstly, it would ensure preparedness across cybersecurity communities; secondly, through information sharing it would provide continuous shared situational awareness;

[485] 'ECSO Position Paper on Sector-Specific ISACs' (*ECSO,* 2018) 11-12.
[486] ibid.
[487] Joint Communication to the European Parliament and the Council- The EU's Cybersecurity Strategy for the Digital Decade [2020] JOIN 18 final 6-7.
[488] ibid.
[489] ibid., 13-14.
[490] ibid.
[491] ibid.
[492] ibid.

> thirdly, it would reinforce coordinated response and recovery. To achieve these objectives, the Unit should build on well-defined blocks and goals, such as guaranteeing secure and rapid information sharing, improving cooperation among participants, including interaction between Member States and relevant EU entities, establishing structured partnerships with a trusted industry base and facilitating a coordinated approach to cooperation with external partners. In order to do so, based on a mapping of available capabilities at national and EU level, the Unit could facilitate the development of a cooperation framework.[493]

As of the writing of this report, the JCU proposal is still in its early stages and sets out further steps that are needed to bring the JCU to fruition. These include the need to '*define*, by mapping available capabilities at national and EU level' and to '*prepare*, by establishing a framework for structured cooperation and assistance.'[494]

Cyber Shield and JCU Implications for Incident Reporting

The Cyber Shield and the JCU are thus expected to greatly mitigate existing issues regarding information sharing and incident handling. The Cyber Shield also looks to centralise incident reporting for SCOs. It is one of the SOCs' many responsibilities to report incidents based on their 'signal and pattern identification and threat knowledge extraction from the large quantities of data' pertinent to the organisation to which they are attached.[495] However, there is more to be done with respect to harmonising incident reporting. The Commission's proposals for both the Cyber Shield and the JCU, as outlined in the 16 December 2020 communication, do not discuss how existing incident reporting frameworks might be revamped to better reinforce these new frameworks and be integrated with them. By indicating that the JCU 'could facilitate the development of a cooperation framework,'[496] without specifying at this stage how this might be done, the new Cybersecurity Strategy leaves open the question of what such a cooperation framework might look like. Following a consideration of the Commission's proposed revision of the NIS Directive and its proposed regulations for the financial sector, this section puts forward further suggestions about what the elements of such a cooperation framework might look like.

---

[493] Joint Communication to the European Parliament and the Council- The EU's Cybersecurity Strategy for the Digital Decade [2020] JOIN 18 final 13-14.
[494] ibid.
[495] ibid., 6-7; Juliana De Groot, 'What is a Security Operations Center (SOC)?' (*Digital Guardian*, 25 November 2020) <https://digitalguardian.com/blog/what-security-operations-center-soc> accessed 20 December 2020.
[496] Joint Communication to the European Parliament and the Council- The EU's Cybersecurity Strategy for the Digital Decade [2020] JOIN 18 final 13-14.

NIS Directive II and Cross-Border Information Sharing

The Commission's proposed NIS revision also puts forward a number of measures that would reinforce cross-border information sharing. Article 26 requires member states to facilitate 'cybersecurity information sharing arrangements', which 'essential and important entities' can join or leave as appropriate.[497] ENISA is tasked with developing guidelines for these agreements, but the formation of such arrangements has a degree of flexibility.[498]

Such arrangements would facilitate information sharing with appropriate tailoring to a given group of relevant entities and authorities. However, such arrangements would not constitute a centralised incident reporting, analysis, information sharing, and advisory cyber hub of the type that has previously been raised by some in the policy literature and which is discussed later in this section.

Neither would the Commission's proposed reinforcements to the CSIRTs Network. While the proposed revision document strengthens the CSIRTs Network's capabilities, including with respect to coordinated vulnerability disclosure and working closely with Security Operations Centres, the CSIRTs Network's broader framework of horizontal information exchange and cross-border cooperation remains much the same, with the various single points of contact 'forwarding incident notifications' to one another.[499]

The revision's creation of the European Cyber Crises Liaison Organisation Network (EU-CyCLONe) is a more concerted effort 'to ensure the regular exchange of information among Member States and Union institutions, bodies and agencies.'[500] Its roles include:

> (a) increasing the level of preparedness of the management of large-scale incidents and crises; (b) developing a shared situational awareness of relevant cybersecurity events; (c) coordinating large scale incidents and crisis management and supporting decision-making at political level in relation to such incidents and crisis; (d) discussing national cybersecurity incident and response plans referred to in Article 7(2).[501]

EU-CyCLONe can thus be seen as providing cross-border information sharing, incident analysis, and incident handling functions similar to those of the CEPS-ECRI and EBF cyber hub ideas

[497] NIS Directive II Art. 26.
[498] NIS Directive II Art. 26.
[499] NIS Directive II 10, 17.
[500] NIS Directive II Art. 14.
[501] NIS Directive II Art. 14.

discussed later in this section. The revision does not give EU-CyCLONe the characteristics of an EU-level cyber incident reporting hub, however. In this and other respects, its relationship with the CSIRTs Network is still to be defined, with the current statement on this relationship being that 'EU-CyCLONe shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements.'[502] This paper's EU-level cyber hub suggestions offer possible components for that relationship.

NIS Directive II and Incident Reporting Harmonisation

The revised NIS Directive II is conscious of incident reporting fragmentation, however, and puts forward some measures to mitigate the situation. It proposes establishing a 'single entry point' in each member state for notifications under various frameworks, in light of the following considerations:

> Essential and important entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional burdens and may also lead to uncertainties with regard to the format and procedures of such notifications. In view of this and, for the purposes of simplifying the reporting of security incidents, Member States should establish a single entry point for all notifications required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC. ENISA, in cooperation with the Cooperation Group should develop common notification templates by means of guidelines that would simplify and streamline the reporting information requested by Union law and decrease the burdens for companies.[503]

The proposed revision thus helps to mitigate the issue of multiple incident reporting frameworks highlighted in the revision document and in Section III.I. by reducing complication at the national level. This is a significant improvement to incident reporting in the EU.

However, the extent to which these 'single entry point[s]' will reduce the multiplicity of incident reporting frameworks is not entirely clear. In stipulating that the 'single entry point' would also be used for incident reporting 'under other Union law', but also particularising '*such as* Regulation (EU) 2016/679 and Directive 2002/58/EC' (own emphasis), it is unclear how

[502] NIS Directive II 20, Art. 14.
[503] NIS Directive II 24.

comprehensively the 'single entry point' would draw together the six incident reporting frameworks outlined in Section III.I. In addition,

> This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.[504]

This includes a separate incident reporting framework for the financial sector, discussed shortly.

The extent to which the 'single entry point' efficiently centralises incident reporting is further called into question where Article 20 stipulates that 'Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities *or* the CSIRT' (own-emphasis).[505] The revision accounts for the situation '[w]here the CSIRT did not receive the notification', in which case advice to the entity 'shall be provided by the competent authority in collaboration with the CSIRT.'[506] That both the competent authorities and the relevant CSIRTs can be distinct from the single point of contact is indicated in the statement that '[a]t the request of the competent authority or the CSIRT, the single point of contact shall forward notifications received pursuant to paragraphs 1 and 2 to the single points of contact of other affected Member States.'[507]

While the proposed revision also specifies that 'entities falling outside the scope of this Directive may submit notifications, on a voluntary basis, of significant incidents, cyber threats or near misses' (which helps to further reduce fragmentation),[508] there remains room for further mitigation of incident reporting fragmentation.

Special Case for the Financial Sector

That being said, more concerted efforts are being made to develop a special and improved incident reporting framework for the financial sector at the EU-level, as well as particular regimes for distributed ledger technologies and markets in crypto-assets within that sector.

[504] NIS Directive II 15.
[505] NIS Directive II Art. 20.
[506] NIS Directive II Art. 20.
[507] NIS Directive II Art. 20.
[508] NIS Directive II Art. 27.

With respect to the 'pilot regime for market infrastructures based on distributed ledger technology', incident reports are to be made to the competent authorities and ESMA.[509] In addition,

> ESMA shall fulfil a coordination role between competent authorities, with a view to building a common understanding of distributed ledger technology and DLT market infrastructure as well as a common supervisory culture and convergent supervisory practices, ensuring consistent approaches and convergence in supervisory outcomes.[510]

The Commission's proposal for a regulation on Markets in Crypto-assets also has competent authorities work closely with one another and with the EBA and ESMA.[511]

Referring to the financial sector more broadly, the revised NIS Directive states that a forthcoming framework for the financial sector should hold precedence for that sector vis-à-vis the revised directive and that 'Member States should therefore not apply the provisions of this Directive on cybersecurity risk management and reporting obligations, information sharing and supervision and enforcement to any financial entities covered by Regulation XXXX/XXXX.'[512] This yet-to-be confirmed regulation would overlap with national frameworks in the following ways:

> The competent authorities under Regulation XXXX/XXXX should transmit details of major ICT-related incidents also to the single points of contact designated under this Directive. Moreover, Member States should continue to include the financial sector in their cybersecurity strategies and national CSIRTs may cover the financial sector in their activities.[513]

A preliminary proposal for such regulation on 'digital operational resilience for the financial sector' was released on 24 September 2020, which promotes 'voluntary information sharing arrangements', similar to those raised in Article 26 of the Commission's proposed revision of the

[509] Proposal for a Regulation of the European Parliament and of the COUNCIL on a pilot regime for market infrastructures based on distributed ledger technology COM(2020) 594 final Art. 9.
[510] ibid.
[511] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 COM(2020) 593 final Title VII.
[512] NIS Directive II 15.
[513] NIS Directive II 15.

NIS Directive.[514] The 24 September draft also proposes that the idea of an EU-level financial sector reporting hub be further investigated. Specifically, that:

> The ESAs, through the Joint Committee and in consultation with ECB and ENISA, shall prepare a joint report assessing the feasibility of further centralisation of incident reporting through the establishment of a single EU Hub for major ICT-related incident reporting by financial entities. The report shall explore ways to facilitate the flow of ICT-related incident reporting, reduce associated costs and underpin thematic analyses with a view to enhancing supervisory convergence.[515]

The 24 September proposal notes that such a hub could take two-different forms, namely 'by means of a single central EU Hub either directly receiving the relevant reports and automatically notifying national competent authorities, or merely centralising reports forwarded by the national competent authorities and fulfilling a coordination role.'[516] The due date for the joint report is expected to be '3 years after the date of entry into force' of the proposed regulation.[517] Until such a hub is further assessed, 'ICT-related incident reporting should be harmonised for all financial entities by requiring them to report to their competent authorities only'.[518]

In relation to the draft regulation's proposal regarding a cyber hub for the financial sector and in light of prior policy proposals by CEPS-ECRI and the EBF, this paper puts forward some suggestions about how such a hub might operate. This paper suggests a framework where the hub is the first point-of-contact for significant financial institutions but receives reports from other financial institutions through national single points-of-contact at the discretion of those authorities.

ii. Existing EU-Level Cyber Hub Proposals

While all of the aforementioned revisions significantly improve the harmonisation of incident reporting and information sharing in various, mutually reinforcing ways, the Cyber Shield, the JCU, and the revised NIS framework stop short of an EU-level cyber hub of the type discussed below. Where the idea for a finance-sector-specific hub is raised in the 24 September proposal, it is to state that the possibility should be researched further, with only an abstract outline of what

[514] Proposal for a Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 COM(2020) 595 final 19.
[515] ibid., Art. 19.
[516] ibid., 21.
[517] ibid., Art. 19.
[518] ibid., 21.

aspects need to be researched at this stage. Considering the merits of pan-sectoral and finance-sector-specific hubs that have been raised by the 2018 CEPS-ECRI Task Force and the 2019 EBF report on incident reporting, the following discussion engages with and builds on this existing literature to put forward suggestions for improving incident reporting at both the national and international levels. It considers how a new pan-sectoral, EU-level entity known as a cyber-hub could bring reporting streams closer together and facilitate more harmonised incident reporting across the members of the JCU. Such an entity would build on the CSIRTs Network and work closely (and potentially integrate) with the Cyber Shield, a potential cyber vulnerability repository, and EU-CyCLONe to facilitate rapid information sharing, data analysis, and incident handling. It would also work closely with ISACs. In view of the practicalities of establishing such a pan-sectoral hub at this stage, this paper then focuses its suggestions on a cyber hub framework for the financial sector. It finally turns to the topic of reporting templates.

Both the 2018 CEPS-ECRI and the 2019 EBF reports emphasise the need for efficient legislative and institutional frameworks for incident reporting and information sharing in view of the existing fragmentation at the time of their writing (see Section III.I. for a discussion of these issues).[519] These issues have been heightened by a lack of standardised terminology across the member states, though this issue of standardisation will be mitigated somewhat by the Commission's proposed revision of the NIS Directive.[520] To rectify the situation, the CEPS-ECRI Task Force and EBF have suggested establishing a European Cyber Hub.[521] This hub is envisioned as a central organisation that would collate and analyse information about cybersecurity incidents. It would use this information to advise CSIRTs and equivalent authorities established by other EU-level reporting frameworks. It would satisfy the need to 'develop further a cross-border framework that facilitates the exchange of information and electronic evidence for the purpose of prevention, investigation and attribution of cross-border cybercrimes.'[522] Crucially, such a hub would issue guidance to CSIRTs and organisations in response to a given incident report.[523]

[519] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 13-14; European Banking Federation, 'EBF Position Paper on Cyber Incident Reporting' (2019).
[520] NIS Directive II Art. 10(4), Art. 22; Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 13-14.
[521] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the policy mix right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 4, 12-13; European Banking Federation, 'EBF Position Paper on Cyber Incident Reporting' (2019) 7-8.
[522] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 4.
[523] ibid., 14.

The extended CEPS-ECRI vision for a hub—which is similar to that of the EBF[524]—reads:

> A hub should be developed with the objective of centralising all incident reports and dispatching them to the right authorities. The hub could be in charge of incident reporting for the whole financial sector and handle relationships with all concerned authorities, regardless of whether these authorities are national or European. It could cover all sectors. Alternatively, hubs specific to the financial sector could be developed. In return, the hub would be in charge of informing and advising financial firms on cyber-incidents. By centralising all incident reports for the financial sector, the hub would have a broad and clear picture at any given time of the cyber-risks in this sector. Strong analytical capabilities would be needed in this respect. The purpose would not be to have a hub that is only a dispatcher of incident reports. The hub could also play the role of coordinator between, on the one hand, all authorities in charge and, on the other hand, authorities and CSIRTs.[525]

iii. Additional European Cyber Hub Observations and Suggestions

Given the new EU Cybersecurity Strategy and the Commission's proposed revision of the NIS Directive, the coordinating role described above could take the form of drawing together the national single points-of-contact, as well as other relevant entities involved in the JCU and Cyber Shield, into a closer relationship that facilitates more reliable incident reporting. This would, in turn, reinforce the revamped information sharing mechanisms proposed by the Commission.

- With EU-CyCLONe expected to be a coordinator for cross-border information sharing and incident handling, a pan-sectoral cyber hub could be composed of EU-CyCLONe and an incident reporting arm/hub that provides complementary coordination of incident reports. Both parts of the wider cyber hub could work closely together to analyse ongoing incidents and advise CSIRTs.

- With the JCU being a 'backstop where the participants can draw on one another's support and expertise' rather than 'an additional, standalone body',[526] such a wider cyber hub could serve as the JCU's coordinating body for incident reporting, analysis, handling,

[524] European Banking Federation, 'EBF Position Paper on Cyber Incident Reporting' (2019) 7-8.
[525] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 15.
[526] Joint Communication to the European Parliament and the Council- The EU's Cybersecurity Strategy for the Digital Decade [2020] JOIN 18 final 14.

and information sharing, that draws together the CSIRTs Network and the EU Cyber Shield. It would also work closely with ISACs and the Critical Entities Resilience Group.

- The hub could also cooperate with TIBER-EU, the ECB, the SSM, the Euro Cyber Resilience Board, national governments, and Europol on resilience building and incident handling in the financial sector.

- The cyber hub's incident reporting component would provide more centralised coordination between the national single points-of-contact of affected member states, particularly where the same incident is being reported in different member states at the same time. As a central receiver and 'dispatcher of incident reports',[527] this component could efficiently identify where various reports from across the union relate to the same incident and could work with EU-CyCLONe to advise CSIRTs accordingly.

- Entities across various regulatory frameworks that are deemed to have cross-border significance could be required to report directly to the EU-level hub, with reports from other entities being directed to the relevant institutions at the national level. National institutions could forward the latter type of report to the EU-level hub as appropriate.

- The suggested EU-level coordinator of incident reports would offer an online reporting form that in addition to being sent to the EU-level hub, can at the same time be automatically sent to relevant single points-of-contact and other competent authorities and CSIRTs. In so far as the reporter is aware of which of these entities should be informed, they would be able to select the relevant entities in the form.

  Automatic sharing is one of the options highlighted in the proposed regulation for digital operational resilience in the financial sector with respect to a cyber hub for the financial sector.[528] This paper prefers the automatic sharing option—both for a pan-sectoral and a financial-sector-specific cyber hub—as opposed to 'merely centralising reports forwarded

[527] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 15.
[528] Proposal for a Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 2020/0266 (COD) 21.

by the national competent authorities and fulfilling a coordination role.'[529] Automatic sharing ensures that all relevant authorities receive the report at the same time.

- Drawing on the 2018 CEPS-ECRI, 2019 EBF, and 2009 ENISA proposals,[530] this hub could advise relevant institutions and share (potentially anonymised) incident reports where appropriate. In addition to analysing and reacting to individual reports, the cyber hub would work with ENISA, the Cyber Shield, and various other participants of the JCU to conduct wider analysis of incident reporting across the EU. The cyber hub would work closely with these entities to conduct the qualitative and statistical analyses recommended in the 2009 ENISA paper.

- Further to the NIS revision's efforts to develop a common taxonomy,[531] the proposed cyber hub would work with the other relevant entities to harmonise templates and taxonomies for its participants.

Pan-Sectoral versus Sector-Specific

As indicated above, this paper recognises the desirability of a pan-sectoral hub. While a pan-sectoral approach could be facilitated by the forthcoming EU Cyber Shield, the JCU, a cyber vulnerability repository (see Sections III.III. and IV.III.), and EU-CyCLONe, it is uncertain whether there will be the inclination in the near to mid-term future to dedicate the magnitude of resources such a project would require, especially given that the EU already looks to invest significant resources in the new cybersecurity initiatives discussed previously. The €1.7 billion earmarked for various cybersecurity areas over the next seven years may facilitate the beginning of a pan-sectoral approach which falls within the Digital Europe Programme's aim to '[s]upport the wide deployment of the cybersecurity capacities across the economy.'[532] However, that €1.7 billion must be shared between four broad areas of cybersecurity across 2021-2027 (see Sub-section II.xxi.), such that a less ambitious cyber hub may be more appropriate at this time.

[529] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!–Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 15.
[530] Vangelis Ouzounis, 'Good Practice Guide on Reporting Security Incidents' (*ENISA,* 2009) 56-62, 69; Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!–Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 14-15; European Banking Federation, 'EBF Position Paper on Cyber incident reporting' (2019) 7; 'ECSO Position Paper on Sector-Specific ISACs' (*ECSO,* 2018) 11.
[531] Vangelis Ouzounis, 'Good Practice Guide on Reporting Security Incidents' (*ENISA,* 2009), 47, 69; European Banking Federation, 'EBF Position Paper on Cyber Incident Reporting' (2019) 7; Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!–Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 12-13.
[532] 'EU Budget for the Future' (*European Commission*, 2020).

While this paper encourages the idea of a pan-sectoral hub so as to better analyse and handle hybrid incidents and cross-sectoral risk, the following suggestions focus and build on the concept of a cyber hub for the financial sector. Given that the €1.7 billion will be divided across four cybersecurity areas, a cyber hub for the financial industry will be more practically and politically feasible than a pan-sectoral one, especially if it consists only of those institutions that are most likely to trigger systemic instability if compromised by a cyber incident. Efforts in this direction can build on the momentum towards the Digital Single Market and the growing attention to cyber-induced systemic risk while being more acceptable to those wary of greater centralisation. At the same time, these efforts can set the stage for a future pan-sectoral hub.

Therefore, in view of the Commission's proposed regulation on ICT incidents in the financial sector, the EU could first *establish a cyber hub composed primarily of those financial institutions that might propagate security issues and financial instability across borders* due to a cyber incident.

- Financial institutions above a given asset value and cross-border presence could be required to report incidents directly to the financial cyber hub. National points-of-contact could share incident reports from other financial institutions with this hub at their discretion. This dual approach would facilitate the rapid analysis and handling of cross-border risk while leaving matters of less-contagious national security to member states.

- The 'significant' institutions would include the 115 banks identified as such by the ECB on the basis of asset size, 'economic importance', cross-border presence, and 'direct public financial assistance'.[533] These institutions are under the ECB's direct supervision through the Single Supervisory Mechanism (SSM).[534]

- The collective cyber hub for 'significant' financial institutions would work in close cooperation with EU-CyCLONe, the EU Cyber Shield, the CSIRTs Network, a cyber vulnerability repository, and other relevant institutions.

[533] 'What makes a Bank Significant?' (*European Central Bank*) <www.bankingsupervision.europa.eu/banking/list/criteria/html/index.en.html> accessed 27 December 2020.
[534] 'Single Supervisory Mechanism' (*European Central Bank*) <www.bankingsupervision.europa.eu/about/thessm/html/index.en.html> accessed 20 September 2020.

- Given that attacks on financial institutions could be made in concert with attacks on other infrastructures (i.e., hybrid attacks),[535] key firms or operators in other sectors that have a particularly close relationship with the financial sector might join the financial cyber hub on a case-by-case basis so as to provide and receive quick access to relevant information. Those non-financial entities would simultaneously route reports about incidents that occur on their end through the CSIRTs Network and/or other applicable framework(s).

Other Potential Aspects of a Pan-Sectoral or Financial Cyber Hub

Zero-day vulnerabilities. Proposals for cyber reporting hubs have tended to be framed in terms of reporting incidents. Section IV.III. suggests that affected system providers, or external vulnerability discoverers (following a set period of non-communication from a system provider upon first reporting the vulnerability to that system provider), could report vulnerabilities to the EU-level hub. Including a framework for normalising the rapid, anonymous sharing of information about zero-day vulnerabilities could help to make other firms aware of unidentified zero-day vulnerabilities in their own systems in good time. See Sections III.III. and IV.III. for more on Coordinated Vulnerability Disclosure (CVD), and Sub-section IV.III.vi. for how vulnerability reporting and information sharing at the EU-level might be implemented in relation to an EU-level cyber hub and the revised NIS Directive's provisions for national CVD coordinators and an EU-level vulnerability repository.

Cyber insurance. As discussed in Section III.VI., this is an emerging market. Intrinsic issues like information asymmetry and adverse selection are exacerbated in the cybersecurity context.[536] As a 2019 Bruegel paper notes, better information sharing can help to reduce these issues.[537] So can statistical analyses. An EU-level cyber hub's reinforcement of both information sharing and statistical analyses, in conjunction with EU–CyCLONe and other members of the JCU, would facilitate stronger cyber insurance.

Decentralised technologies. Reporting and handling incidents that occur on decentralised fintech is particularly tricky and may benefit from a dedicated entity/hub/consortium that specialises in such incidents and works closely with a general cyber hub. The intrinsic ambiguity about

[535] Maria Demertzis and Guntram Wolff, 'Hybrid and Cybersecurity Threats and the European Union's Financial System' (*Bruegel,* 2019).
[536] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018), 19; Maria Demertzis and Guntram Wolff, 'Hybrid and Cybersecurity Threats and the European Union's Financial System' (*Bruegel,* 2019) 11.
[537] Maria Demertzis and Guntram Wolff, 'Hybrid and Cybersecurity Threats and the European Union's Financial System' (*Bruegel,* 2019) 11.

controllers and processors in decentralised fintech makes it more difficult to comply with the GDPR and efficiently report and handle incidents.[538] This characteristic also makes it more challenging to allocate responsibility for patching and handling and to enforce security standards.

An entity that has a view of decentralised components of the financial system and that receives reports about vulnerabilities and incidents in decentralised fintech could issue guidance on responsibility and liability regarding decentralised components of the financial system. As such an entity builds up oversight and incident analysis capacity, the entity could help to identify key actors involved in decentralised systems whose roles and relationships may not be apparent until an incident runs its course. An entity that uses its knowledge of the opensource systems within its remit to help identify actors could reduce confusion and contention about cybersecurity responsibility. Such an entity that has a view of decentralised components of the financial system and interfaces with a wider cyber hub would be able to provide guidance on incidents and vulnerabilities in decentralised parts of the financial system. Building on initiatives already proposed or undertaken in the EU, Section IV.V. discusses such an entity in greater detail.

iv. Suggestions for Incident Reporting Templates

Whether or not an EU-level cyber hub is established, it is important to have effective reporting templates and convenient ways of submitting those templates. While it is essential to account for the diversity of different financial technologies and systems when developing templates, it is also vital to reduce fragmentation and to create greater standardisation. In addition, the information prompts should be appropriately detailed and easy to access. As indicated in Sub-section III.I.v., templates have ranged from online forms to emails, with varying degrees of prompts for technical details that reflect the character of specific sectors and sub-sector groups.

The Commission's proposed revision of the NIS Directive stipulates that 'ENISA, in cooperation with the Cooperation Group should develop common notification templates by means of guidelines that would simplify and streamline the reporting information requested by Union law and decrease the burdens for companies.'[539] This paper puts forward suggestions about what such templates might look like. The following suggestions for reporting templates offer greater harmonisation and ease of cooperation while being applicable to both more and less centralised frameworks.

[538] cf. GDPR Rec. 73, 86-88, Art. 34.
[539] NIS Directive II 24.

This paper suggests that national 'single entry point[s]' and a potential EU-level hub could offer *a common online form filtered by relevant regulatory frameworks and the affected sector and sub-sector group(s).*

- This form could expand to display a set of sector and sub-sector specific questions once the reporter specifies the sector and sub-sector to which they belong. National points-of-contact should work closely with one another and with sectoral representatives to develop these tailored prompts in line with guidelines and regulations that apply to a given sector and member state.

  The online reporting form could ask for details regarding a reporting (financial) institution's relationship with other financial institutions and operators of essential services. Given the possibility of systemic instability triggered by unusually large, interconnected, or hybrid events, reporting categories and forms that take the extent of the financial sector's integrated nature into account can help to improve resilience and robustness. An aspect of doing so would be to provide fields for identifying relevant third+ parties.

  The Monetary Authority of Singapore's (MAS) template may offer a useful example for reporting cyber incidents in the financial sector (see Appendix iii).

- Rather than expanding the number and detail of prompts at a later stage (see Appendix i for ENISA's template guideline in the eIDAS context, which describes 'an initial and short description of the incident' for the first stage; see also Appendix iii for MAS's approach), the suggested form could prompt for the full range of relevant (sub)sector-specific information and technological detail at every stage. Indeed, the NIS Directive stipulates a two-stage approach, but it would be better to tailor the number of stages depending on the incident. While a reporter would not have to fill in all the prompts at every stage—potentially putting TBC ('to be confirmed') for fields that they cannot answer at a given time—providing the prompts in full would facilitate the capture of as much pertinent information at each incident reporting stage as possible.

The multi-stage approach advocated in this paper echoes that of the Commission's proposed regulation on 'digital operational resilience for the financial sector' but contrasts with that of the

revised NIS Directive (see Sub-section III.I.v.).[540] The latter stipulates a two-stage approach, with a brief first incident report and a more detailed follow-up report.[541] The revised NIS Directive further stipulates that '[t]he initial notification should only include the information strictly necessary to make the competent authorities aware of the incident and allow the entity to seek assistance, if required.'[542]

Taking into account that cyber incident reports beyond the financial sector can have a bearing on the security and stability of the financial system, this paper suggests that there is merit to normalising regular intermediate reporting stages for any incidents that have a long-duration or take a long-time to assess after they have run their course.

With respect to template content, the Commission's proposed regulation on 'digital operational resilience for the financial sector' requires 'common draft regulatory technical standards' and 'common draft implementing technical standards' to be developed within a year of the proposal's ratification.[543] The draft regulation does not address the detail required in each incident reporting stage, however.

This paper sees merit in templates that provide thorough prompts at each reporting stage so that as much pertinent information as possible is likely to be captured at any given stage. This need not significantly slow down the early incident report(s), since the reporter would not be required to fill in all the fields at every stage. At the first stage, they could be required to fill in certain fields while having the option of responding to others.

[540] Proposal for a Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 COM(2020) 595 final; NIS Directive II 23.
[541] NIS Directive II 23.
[542] ibid.
[543] Proposal for a Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 COM(2020) 595 final; NIS Directive II 23.

IV.II. THIRD-PARTY+ OVERSIGHT

With banks increasingly reliant on third-party+ services, financial institutions need to be secure in the knowledge that third parties and their sub-contractors are not cybersecurity risks. Contractors anywhere in the service chain have a responsibility to conduct proper oversight on the companies they contract. Per GDPR, for example, a controller is expected to ensure that it and its processors comply with GDPR's data protection standards.[544]

As discussed in Section III.II.iv., the 24 September proposal on 'digital operational resilience for the financial sector' would significantly strengthen the oversight of critical third-party+ service providers. The draft proposal stipulates more stringent security requirements for critical third parties, oversight responsibilities for financial institutions, and the establishment of an Oversight Forum and a Lead Overseer for supervising critical third parties. These measures significantly mitigate the issue identified in Section III.II.iii., which concerns controllers being able to retroactively gain compensation from processors for the processors' part in an incident without the extent of a controller's ability to do so being explicitly dependent on the quality of their own instructions and oversight. Even with the stronger oversight framework that the 24 September proposal outlines for the financial sector, however, it could be worth mitigating this issue in order to reinforce oversight frameworks in a variety of sectors that have a bearing on financial security.

- A *revision of the GDPR provision that allows controllers to claim compensation from culpable processors* could strengthen controllers' incentives for pursuing stricter security standards across their processors. While the idea of joint culpability is an important concept that aligns the interests of processors and controllers in maintaining data security, a revision could *explicitly take into account the quality of oversight*. Doing so could spur controllers to oversee processors' cybersecurity standards more strictly and encourage the proliferation of stricter cybersecurity standards across third-party+ vendors.

[544] GDPR Articles 4, 24, 28.

IV.III. COORDINATED VULNERABILITY DISCLOSURE

Another important aspect of cybersecurity is the identification, reporting, patching, and disclosure of software vulnerabilities before they are exploited by malicious actors. As discussed in Section III.III., security researchers look for vulnerabilities in software systems in order to report them to the affected company/vendor/organisation so that the vulnerabilities can be patched. The ease with which security researchers can report zero-day vulnerabilities—as determined by a vendor's CVD policy—is directly pertinent to cybersecurity.

This section begins by outlining the Dutch national CVD framework, which has been held up as an example for other member states (see Sub-section III.III.iii.). This is followed by a discussion of how to mitigate the issue of CVD quality raised in Section III.III. This section first considers how to foster the widespread development of rigorous CVD policies where the details of such policies are primarily determined at company-level at present. Second, it considers how to improve information sharing where knowledge of a vulnerability may benefit the wider community. Throughout this discussion, there is a consideration of the extent to which various frameworks developed in the US and the Netherlands that have been highlighted by ENISA and CEPS can address these issues.

This paper builds on their observations to suggest:

- *The signing of CVD manifestos at the sectoral and sub-sectoral levels.*
- *Further consolidating vulnerability reporting at the EU-level.*
- *Normalising the rapid sharing of anonymised vulnerability information between relevant parties.*

This paper's CVD suggestions can contribute to the revised NIS Directive's efforts to strengthen and harmonise CVD in Europe. While this paper suggests greater consolidation at the EU-level, some of these suggestions can be productively pursued at the member state and sectoral levels.

i. NIS Directive II and CVD

The Commission's proposed revision of the NIS Directive establishes national CVD 'coordinators' by stipulating that a CSIRT in each member state will serve as 'a trusted intermediary, facilitating, where necessary, the interaction between the reporting entity and the

manufacturer or provider of ICT products or ICT services' (see Sub-section III.III.iii.).[545] Such coordinators will work closely with the CSIRTs Network in cross-border cases.[546] The revised NIS Directive also states that 'CSIRTs shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies' including those for CVD.[547] However, the interactions of such coordinators with reporters and vendors are not set out in detail. For example, what the reporting process to the coordinator might look like and the extent to which some vendors should be required to report vulnerabilities are left to be determined.

In addition to national CVD coordinators, the revised NIS Directive would also institute a European vulnerability registry run by ENISA. The registry can be considered a form of CVD hub at the EU-level in so far as it collates, updates, and makes available information about vulnerabilities that have been submitted to it 'on a voluntary basis' by 'essential and important entities and their suppliers, as well as entities which do not fall in the scope of application of this Directive.'[548] While such a registry will considerably increase the extent to which vulnerabilities are disclosed to a wider audience and also improve the quality of those disclosures, the voluntary approach as outlined in the draft document still comes with the risk that vulnerabilities that should be disclosed are not disclosed. This section thus also considers how to further mitigate this risk, short of requiring all vulnerabilities to be reported to the registry and disclosed publicly.

ii. Harmonisation Based on the Dutch Framework

The Netherlands have been at the forefront of CVD in the EU and offer a well-respected national CVD framework on which other member states might base their own. As highlighted in Sub-section III.III.iii., the policy literature has given considerable attention to this framework.[549] The Dutch National Cyber Security Centre (NCSC) guidelines promote the implementation of CVD policies in organisations.[550] However, the NCSC does not supervise the implementation of CVD policies, nor does it monitor the quality of such policies.[551] If necessary, the NCSC can help to

[545] NIS Directive II Art. 6.
[546] NIS Directive II Art. 6.
[547] NIS Directive II Art. 10(4)(c).
[548] NIS Directive II 19.
[549] 'Coordinated Vulnerability Disclosure: Guidelines published by the NCSC', (*ENISA,* 2018) <https://www.enisa.europa.eu/news/member-states/coordinated-vulnerability-disclosure-guidelines-published-by-ncsc> accessed 3 May 2020; William Phillips, Giacomo Persi Paoli, Cosmin Ciobanu, *Economics of vulnerability disclosure*, (*ENISA*, 2018) 39-41; Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) 23-39.
[550] Rickey Gevers et al., 'Coordinated Vulnerability Disclosure: The Guideline' (*National Cyber Security Centre NL, Ministry of Justice and Security,* 2019) 3; Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018), 26.
[551] Erik Silfversten, et al. *Economics of vulnerability disclosure* (*ENISA,* 2018) 41.

disseminate information about a vulnerability to institutions that might benefit from that knowledge.[552] Where disputes arise between vendors and security researchers, they can seek mediation from the NCSC. For example, '[i]f the reporting of the vulnerability does not go as the reporting party expects, or if they would prefer not to report the vulnerability directly to the organisation, they can contact NCSC'.[553] A 'flow chart of coordinated vulnerability disclosure' within the Dutch Framework is available in CIO Platform Nederland's publication on 'Coordinated Vulnerability Disclosure: Model Policy and Procedure', building on work conducted by Cooperation SURF, the Dutch National Cyber Security Centre and Floor Terra.[554] The case gets handed to the Public Prosecution Authority if authorities deem that the security researcher violated a vendor's CVD policy or used excessive measures to report the vulnerability in cases where a CVD policy is unclear or non-existent.[555]

The Public Prosecution Authority ensures that security researchers comply with existing criminal law. It focuses on three main principles.[556] Firstly, it considers motives. What are the ethical motives of the hacker? Secondly, it considers subsidiarity. To be considered ethical, the hacker should confidentially report their discovery to the party responsible for patching as soon as possible without strings attached. Thirdly, it considers proportionality. If the hacker (intentionally or unintentionally) acts more aggressively than demonstrating the vulnerability warrants, the prosecutor may launch a criminal investigation to determine whether the actions were appropriate.[557] These principles of proportionality and subsidiarity are familiar in EU law.[558] As such, they can serve as a model for other member states' approach to CVD.

iii. Developing Rigorous CVD Policies in the Private Sector

As discussed in Section III.III.iv., a significant issue is how to foster vendors' development of robust CVD policies, given the principle that vendors should be able to determine their CVD policies and that supervision under the revised NIS Directive is *ex post* for important entities.

---

[552] Erik Silfversten, et al. *Economics of vulnerability disclosure* (*ENISA,* 2018) 41; Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) 26.
[553] Rickey Gevers et al., 'Coordinated Vulnerability Disclosure: The Guideline' (*National Cyber Security Centre NL, Ministry of Justice and Security,* 2019) 14.
[554] CIO Experience Group Information Security, 'Coordinated Vulnerability Disclosure: Model Policy and Procedure' (*CIO Platform Nederland*, 2016) 23-24.
[555] ibid., 9.
[556] ibid., 14.
[557] Lorenzo Pupillo, 'Encouraging Responsible Vulnerabilities Disclosure', (*OECD Global Forum on Digital Security for Prosperity*, 2019) 3.
[558] Consolidated version of the Treaty on European Union [2012] OJ C 326 Art. 5.

There is agreement in the policy literature that private sector initiatives can serve as important complements to regulatory frameworks and other government initiatives. ENISA and the 2018 CEPS Task Force on Software Vulnerability Disclosure emphasise the role the private sector should play in the diffusion of robust CVD.[559] While ENISA recognises the importance of government involvement, it argues that 'one of its primary tasks should be to explicitly take a step back and reaffirm that CVD is ultimately a process between security researchers and vendors (and if required, a coordinator).'[560] In general, there is an emphasis on a 'no one-size-fits-all' approach.[561]

The approach to CVD in the US exemplifies private sector freedom. The development of broad-stroke guidelines has included significant private sector involvement.[562] The US Department of Commerce's National Telecommunication and Information Administration (NTIA) initiated a stakeholder consultation on CVD in 2015.[563] Among the products of this initiative are disclosure templates, multiparty disclosure policies, and a commitment to a 'no one-size-fits-all approach'.[564] This consultation inspired other government agencies to develop their own CVD programmes and to issue guidance, including the US Department of Justice's Framework for a Vulnerability Disclosure Program for Online Systems that reaffirms the 'no one-size-fits-all' principle.[565]

---

[559] Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) i, 51; Erik Silfversten, et al. *Economics of vulnerability disclosure* (*ENISA,* 2018) 41; Cosmin Ciobanu, 'Good Practice Guide on Vulnerability Disclosure' (*ENISA,* 2015) 63; Parlour, Richard, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance: Getting the Policy Mix Right!—Report of a CEPS-ECRI Task* Force (Centre for European Policy Studies and European Credit Research Institute, 2018) 18.

[560] Erik Silfversten, et al., *Economics of vulnerability disclosure* (*ENISA,* 2018) 41.

[561] Allen D. Householder, Garret Wassermann, Art Manion, and Chris King, 'The CERT® Guide to Coordinated Vulnerability Disclosure', (*Software Engineering Institute*, 2017) 29-30; Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) 37-38.

[562] Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) vi.

[563] ibid., 37; Angela Simpson, 'Enhancing the Digital Economy Through Collaboration on Vulnerability Research Disclosure' (*National Telecommunications and Information Administration, United States Department of Commerce,* 9 July 2015) <www.ntia.doc.gov/blog/2015/enhancing-digital-economy-through-collaboration-vulnerability-research-disclosure> accessed 11 March 2020.

[564] See preceding citation.

[565] Computer Crime & Intellectual Property Section (Criminal Division), 'A Framework for a Vulnerability Disclosure Program for Online Systems' (*U.S. Department of Justice,* 2017); Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) 37-38; Angela Simpson, 'Enhancing the Digital Economy Through Collaboration on Vulnerability Research Disclosure' (*National Telecommunications and Information Administration, United States Department of Commerce,* 9 July 2015) <www.ntia.doc.gov/blog/2015/enhancing-digital-economy-through-collaboration-vulnerability-research-disclosure> accessed 11 March 2020.

Although there are similar phases for reporting and disclosure across many CVD policy models in the US due to a common baseline established by ISO/IEC 30111 [45] (see Table 2 in 'The CERT® Guide to Coordinated Vulnerability Disclosure' for an outline of common CVD phases in US frameworks), NTIA's recognition that 'no one-size-fits-all' has set a precedent for subsequent initiatives.[566] Therefore, vendors have considerable freedom to develop tailored CVD policies within broad guidelines.[567] The guidelines merely indicate how a vendor might go about developing an unambiguous CVD policy.[568] They stipulate neither necessary objectives nor procedures that a vendor should incorporate into its CVD policy.[569]

The strength of such a decentralised approach is that it facilitates the bottom-up development of strong CVD policies at company level that best fit with vendors' characteristics. However, it also comes with the risk that some vendors will not develop appropriately robust policies. There is thus a need to develop private sector initiatives that balance the benefits of a 'no one-size-fits-all' approach with more concerted efforts to improve common standards within the private sector. The CEPS Task Force encourages business leaders to promote CVD to others in the private sector.[570] Specifically, '[t]he private sector could take the lead in implementing CVD by defining and publishing public reporting mechanisms on vulnerabilities disclosure on companies' websites, according to the ISO standards.'[571]

This paper builds on this private sector emphasis to suggest an approach that, in complement to national CVD frameworks, can both foster vendors' development of high-quality CVD policies and mitigate weaknesses that are latent in *ex post* only supervision approaches. Private sector initiatives that give freedom to the private sector while establishing common standards can

[566] Allen D. Householder, Garret Wassermann, Art Manion, and Chris King, 'The CERT® Guide to Coordinated Vulnerability Disclosure' (*Software Engineering Institute*, 2017) 29-30; Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) 37-38

[567] Computer Crime & Intellectual Property Section (Criminal Division), 'A Framework for a Vulnerability Disclosure Program for Online Systems' (*U.S. Department of Justice,* 2017) 1; Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) vi.

[568] Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) vi.

[569] ibid.

[570] Rickey Gevers et al., 'Coordinated Vulnerability Disclosure: The Guideline' (*National Cyber Security Centre NL, Ministry of Justice and Security,* 2019) 58.

[571] Marietje Schaake, et al., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018) 51.

mitigate *ex post* supervisory weaknesses by facilitating vendors' proactive development of high-quality CVD policies.

Manifesto Initiatives in the Netherlands

The 2016 Amsterdam Coordinated Vulnerability Manifesto is a good example of how sectoral initiatives can reinforce more decentralised approaches to CVD policy development. The Manifesto sets CVD objectives, policies, and processes to which the signatories agree to adhere.[572] Led by CIO Platform Netherlands and Radobank with the support of the Dutch Ministry of Security and Justice, the Manifesto was signed by vendors from across the EU at the High-Level Meeting on Cyber Security in Amsterdam.[573] The meeting occurred during the Dutch Presidency of the European Council, which made digital security a priority.[574] The twenty-nine vendors that signed the Manifesto affirmed their commitment to the CVD objectives, policies and procedures detailed in the Manifesto.[575]

As the number of signatories suggests, however, such vendor-driven initiatives have been limited in their reach thus far. While some signatories like CIOforum Belgian Business connect an extensive network of vendors that may follow their lead,[576] the twenty-nine signatories represent a small fraction of the European economy. Proliferating such initiatives throughout the EU would be a significant step towards mitigating the zero-day vulnerability threat.

iv. Suggestions for Rigorous CVD Policies in the Private Sector

ENISA, national CVD coordinators, and a potential EU-level CVD hub / revamped vulnerability repository (see Sub-section IV.III.vi. for more on a potential EU-level CVD hub) *could encourage the development of manifestos at the sectoral and sub-sectoral levels that contain*

[572] CIO Experience Group Information Security, 'Coordinated Vulnerability Disclosure: Model Policy and Procedure' (*CIO Platform Nederland*, 2016).
[573] 'From the Netherlands Presidency of the EU Council: Coordinated Vulnerability Disclosure Manifesto Signed' (*ENISA,* 2016) <https://www.enisa.europa.eu/news/member-states/from-the-netherlands-presidency-of-the-eu-council-coordinated-vulnerability-disclosure-manifesto-signed> accessed 1 May 2020.
[574] 'From the Netherlands Presidency of the EU Council: Coordinated Vulnerability Disclosure Manifesto Signed' (*ENISA,* 2016) <https://www.enisa.europa.eu/news/member-states/from-the-netherlands-presidency-of-the-eu-council-coordinated-vulnerability-disclosure-manifesto-signed> accessed 1 May 2020; CIO Experience Group Information Security, 'Coordinated Vulnerability Disclosure: Model Policy and Procedure' (*CIO Platform Nederland*, 2016).
[575] Rickey Gevers et al., 'Coordinated Vulnerability Disclosure: The Guideline' (*National Cyber Security Centre NL, Ministry of Justice and Security,* 2019) 5.
[576] 'Coordinated Vulnerability Disclosure Manifesto Signed', (*Radobank,* 2016) <https://www.rabobank.com/en/press/search/2016/20160512-coordinated-vulnerability-disclosure-manifesto.html> accessed 1 May 2020; 'Our Approach', (*Belgian Business CIO Forum*) <https://www.cioforum.be/> accessed 1 May 2020.

sector- and sub-sector-specific objectives, policies, procedures, and template guidelines. In complement to national CVD frameworks, this approach would help to facilitate a baseline CVD quality while respecting the spirit of the 'no one-size-fits-all' approach. It can also balance the governance vulnerabilities of *ex post* only supervision. Manifestos at the sectoral level would allow vendors to ensure that CVD policies fit their distinct sectoral needs and characteristics while establishing a clear standard among signatories. Sectoral subgroups might sign more tailored manifestos to account for the diversity within a given sector.

- Ideally, an entire sector would sign a basic set of objectives, policies, and processes on which the entire sector can agree. A small number of subgroups might sign more tailored manifestos on top of the common standard.
- Even in the absence of a baseline sector-wide manifesto, a constellation of manifestos facilitates an expected set of standards within a subgroup. Those manifestos would serve as a testament to the quality of CVD policies to be found in a given group.
- It is desirable that sectors sign manifestos at the EU-level. Nevertheless, sectoral manifestos at the member state level would be a significant step forward.
- ENISA, national CVD coordinators, and a potential EU-level CVD hub / revamped vulnerability repository could work with business leaders to achieve this framework.

In addition, such a system could be of use to a branch of the nascent cyber insurance market that deals with vulnerabilities. The ease with which ethical hackers are allowed to detect and report zero-day vulnerabilities—as determined by a vendor's CVD policy—are directly pertinent to cybersecurity. Manifestos of groups of vendors with similar types of systems, reporting procedures, and patching policies *can provide relevant information for calculating premiums.*

v. Disseminating Vulnerability Information

As discussed in Section III.III.v., how and when to disseminate information about a vulnerability are also important considerations for cybersecurity.[577] If similar vulnerabilities are present in other vendors' systems, wider disclosure in a timely manner can alert affected vendors and allow them to get ahead of a potential incident. In a highly integrated financial system where similar

[577] CERT Capability Team, 'Good Practice Guide on Vulnerability Disclosure' (*ENISA*, 2015) 9, 59.

vulnerabilities may appear across different financial entities and where cyber-induced systemic instability is a possibility, the benefits of rapid vulnerability disclosure to relevant actors are high.

The US Cybersecurity and Infrastructure Security Agency's (CISA) framework solves the problem of unresponsive system providers by allowing the coordinator to be assertive about information sharing.[578] In the event that a system provider does not acknowledge the receipt of a vulnerability report or 'will not establish a reasonable timeframe for remediation, CISA may disclose vulnerabilities as early as 45 days after the initial attempt to contact the vendor is made.'[579] In this scenario, they can do so whether or not the organisation is working to address the vulnerability.[580] The Dutch NCSC policy sets an expected timeframe for patching and releasing a report at about sixty days. However, in an integrated financial system, sixty or even forty-five days is a long time before other potentially affected vendors can begin working on a patch, especially if they have a similar but not identical vulnerability that cannot be solved through the same patch. The following suggestions aim to facilitate and normalise rapid, ongoing information sharing at the EU-level.

vi. Suggestions for Consolidating CVD and Normalising Wider Disclosure

This paper suggests *further consolidating vulnerability reporting at the EU-level.*

- As intimated in Section IV.I.iii., the competencies of the Commission's proposed vulnerability repository could potentially be expanded into an EU-level CVD hub that handles vulnerability reports that are regularly passed to it from the national CSIRTs in charge of CVD, as well as reports that are submitted directly. Alternatively, one of the wider EU-level reporting hubs suggested in Section IV.I. (whether pan-sectoral or financial) could serve such a function, working closely with the potential vulnerability repository to make information about vulnerabilities available to relevant entities at appropriate times and to an appropriate extent.

- Whether or not a potentially revamped vulnerability repository or a potential EU-level cyber hub are implemented, vendors could send reports to the relevant coordinator in multiple stages as their investigation into a vulnerability and efforts to patch it are ongoing.

[578] CERT Capability Team, 'Good Practice Guide on Vulnerability Disclosure' (*ENISA*, 2015) 9, 59.
[579] ibid.
[580] 'CISA Coordinated Vulnerability Disclosure (CVD) Process' (*Cybersecurity and Infrastructure Security Agency, Department of Homeland Security,* 3 December 2019) <www.cisa.gov/coordinated-vulnerability-disclosure-process> accessed 28 April 2020.

An online reporting system could automatically send a notification to the security researcher (whose contact details the vendor would submit in the initial online reporting form) informing the researcher that the coordinator has been contacted. If a vendor does not submit an initial report within a set period, the security researcher could report to the hub/repository/coordinator, potentially after having first sought to follow-up with the vendor. The multi-stage reporting process could resemble the incident reporting framework suggested previously. Significance criteria could be used to determine which vendors are required to submit reports to the coordinator upon the discovery of a vulnerability. Where a vendor is not on the list of those required to report vulnerabilities, the security researcher might also have the option of contacting the coordinator directly about a vulnerability if they have reason not to contact the vendor first.

This paper also suggests *normalising a rapid, ongoing information sharing system.*

- Time-sensitive vulnerabilities that may be found elsewhere in the financial sector or other relevant sectors could be (anonymously) shared between institutions participating in an EU-level financial cyber hub while the organisation(s) in initial receipt of the vulnerability report(s) are still patching their system(s). This approach would allow other affected institutions to start patching as soon as possible (as similar vulnerabilities in different systems might not be easily solved with the same patch). It would also help to mitigate any systemic implications while preserving anonymity (if desired and appropriate) and restricting the sphere of attention during the critical stage. This could similarly be done beyond the financial sector by developing one of the multi-sectoral, EU-level hub/repository options suggested above.

- Normalised information sharing does not mean that the EU-level hub/repository would disseminate information on all vulnerabilities automatically. In consultation with the reporter, affected system provider, and relevant national CSIRTs, they could determine whether and with whom to share these multi-stage reports. This group of actors would also consult with one another to decide whether to keep the participants anonymous and whether there is any other information that should be kept confidential. The possibility to remain anonymous is likely to make participation in the hub/repository more attractive

than otherwise.[581] Normalised sharing means that sharing would be an expected, if not always utilised, element of the framework.

Such normalisation would be an instance of 'information-sharing arrangements that protect the potentially sensitive nature of the information shared, and that are governed by rules of conduct in full respect of business confidentiality, protection of personal data and guidelines on competition policy' as per Article 40 of the Commission's proposed regulation on 'digital operational resilience for the financial sector'.[582]

This approach would mitigate the issue of unresponsive vendors and of vendors that keep the patching timeframe ambiguous and would allow other affected vendors to begin patching their systems at an earlier stage. This approach would also reduce the likelihood that a security researcher will disclose the vulnerability publicly without the system provider's consent, since the researcher will know that the hub/repository will share the information within an appropriate timeframe.

[581] 'ECSO Position Paper on sector-specific ISACs' (*ECSO,* 2018) 11.
[582] Proposal for a Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 COM(2020) 595 final Art. 40.

IV.IV. IMPROVING THE RELATIONSHIP BETWEEN LAW AND TECH

As discussed in Section III.IV., emerging financial technologies and regulations can challenge one another in ways that undermine financial cybersecurity. Cooperation between regulators and fintech companies to reduce the tensions in the law and tech relationship is crucial. This section explores ways of improving that relationship. It focuses on the review cycles of existing standards and regulations as well as the status of regulatory sandboxing in the EU.

The suggestions put forward in this section include,

- More frequent reviews of the relationship between various emerging financial technologies and relevant cybersecurity regulations and certification frameworks.
- Aspects of the federal regulatory sandbox bill that is pending in the United States House of Representatives could serve as inspirations for an EU-level sandboxing framework.

i. Regulatory Agility Suggestions

The following suggestions focus on the review cycle for the European cybersecurity certification framework, which is informed by the regulations that pertain to cybersecurity.[583] It is also the scheme that most directly touches on the compliance of technologies with existing cybersecurity requirements requisite for certification. The conclusions of ENISA's review of the certification framework can inform the reviews of existing legislation. This paper suggests review cycles similar to those of the Commission's proposed regulation on 'a pilot regime for market infrastructures based on distributed ledger technology' (see Section III.IV.i.), which has annual evaluations nested within five-year reviews.[584]

Annual evaluations of emerging technologies and their relationship with existing standards by ENISA in close cooperation with the relevant European supervisory authority's (ESA) fintech working group/hub (i.e., those of the Securities and Markets Authority, European Banking Authority, and European Insurance and Occupational Pensions Authority) could help to mitigate vulnerabilities that arise from the disjunction between emerging technologies and legislation.

An annual evaluation cycle would help to keep the regulatory and emerging technologies landscapes in closer relation. The shorter timeline need not result in a rushed evaluation, since

[583] Sławek Górniak, 'ENISA in the EU Cybersecurity Certification Framework' Presentation at the IHE Europe Symposium (Rennes, 9 April 2019).
[584] Proposal for a Regulation of the European Parliament and of the Council on a Pilot Regime for Market Infrastructures Based on Distributed Ledger Technology COM(2020) 594 final 4.

it would not be a full evaluation of all certification schemes. The annual review's focus would be on new fintech with market relevance and their ability to comply with specific certification schemes. The full evaluation of all certification schemes would take place according to the five-year cycle. Existing public-private stakeholder consultation mechanisms, such as those of the ESAs' fintech working groups /hubs, could be utilised throughout this process.

Where ENISA (in consultation with the ESAs' fintech working groups / hubs) deems that a European regulation related to cybersecurity needs re-evaluation following the suggested annual reviews of existing certification schemes, ENISA would advise the European Commission on aspects to re-evaluate in a given regulation's established review period. Where necessary, ENISA might advise the need for an ad hoc review cycle.

ii. Regulatory Sandboxing Suggestions

As discussed in Sub-section III.IV.ii., closer cooperation between regulators and fintech companies across the EU is desirable. Cooperation through regulatory sandboxing benefits financial cybersecurity by heightening (1) fintech companies' understanding of the security regulations to which they must adhere and (2) regulators' understanding of the unconventional nature of certain emerging technologies (e.g., blockchain, for which it is difficult to identify controllers and processors, thus resulting in a problematic relationship with GDPR).[585] Regulatory sandboxes can reduce legal grey zones and law-tech disjunctions that can lead to system vulnerability when legacy and emerging technologies in financial systems comply with security regulations to differing degrees.[586]

An *EU-wide regulatory sandbox framework* could help to lessen cybersecurity risks that arise from the disjunction between emerging tech and security regulation. Regulatory sandboxing at the supranational level would remove residual cross-border rigidities that would be extant in a lateral harmonisation approach.

One possible model for an EU-level regulatory sandbox framework is *The Financial Services Innovation Act of 2016* (FSIA), legislation introduced to the US House of Representatives in

[585] Luke Thomas, 'The Case for Federal Regulatory Sandbox for FinTech Companies' [2018] 22 NC Banking Instit. 278; European Securities and Markets Authorities, European Banking Authority, European Insurance and Occupational Pensions Authority, 'Report—FinTech: Regulatory Sandboxes and Innovation Hubs' [2018] JC 74 19.
[586] European Securities and Markets Authorities, European Banking Authority, European Insurance and Occupational Pensions Authority, 'Report—FinTech: Regulatory Sandboxes and Innovation Hubs' [2018] JC 74 16.

September 2016 that stalled following opposition from the Office of the Comptroller of the Currency based on the objections outlined and countered in Sub-section III.IV.ii.[587]

Section 3 of the bill suggests that twice a year each government agency 'should publish in the Federal Register a nonexclusive list that identifies 3 or more areas of existing regulation (1) that apply or may apply to a financial innovation; and (2) that the agency would consider modifying or waiving if the agency were to receive a petition under section 6 relating to that regulation.'[588] In line with Section 4, '(e)ach agency shall establish a Financial Services Innovation Office (known as "FSIO") to promote financial innovations and to assist a covered person whose petition has been approved under Section 7.' By involving each government agency, these stipulations involve most sectors of the economy.

According to Section 6, a request for a regulatory sandbox must include 'an alternative compliance strategy' that '(A) would serve the public interest; (B) improves access to financial products or services; and (C) does not present systemic risk to the United States' financial system and promotes consumer protection.'[589] Whilst the agency is considering a given petition, the relevant fintech company has 'safe harbor'. This means that the authorities cannot sanction a fintech company for not complying with existing regulations during this interval.[590] 'Injunctive relief' is an exception to 'safe harbor' in cases where an agency has cause to fear that the given fintech 'presents an immediate danger to consumers or presents a systemic risk.'[591] In such cases, a relevant court can decide to prohibit the fintech company from keeping or introducing their 'product, service, or process' in(to) the market until the agency makes a decision.[592]

A fintech's potential relevance to multiple agencies is accounted for by the close communication, information sharing, and coordination between the FSIOs that are also proposed in Section 4.[593] Section 5 establishes a biannually-convened FSIO Liaison Committee, 'composed of the Director of each FSIO office and a State banking supervisor selected by the Conference of State

[587] Luke Thomas, 'The Case for Federal Regulatory Sandbox for FinTech Companies' [2018] 22 NC Banking Instit. 268.
[588] The Financial Services Innovation Act of 2016 H.R. (114th Cong. 2016) 6118 2-4: 'The term "agency" means each of the Board of Governors of the Federal Reserve System, the Bureau of Consumer Financial Protection, the Commodity Futures Trading Commission, the Department of Housing and Urban Development, the Department of the Treasury, the Farm Credit Administration, the Federal Deposit Insurance Corporation, the Federal Housing Finance Agency, the Federal Trade Commission, the National Credit Union Administration Board, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission.'
[589] The Financial Services Innovation Act of 2016 H.R. (114th Cong. 2016) 6118 Sec. 6, 9.
[590] ibid., Sec. 6, 10.
[591] ibid., Sec. 6, 10.
[592] ibid., Sec. 6, 10.
[593] ibid., Sec. 6, 4.

Bank Supervisors (or a successor organisation).'[594] The FSIO representatives chair the committee on a rotational basis with two-year terms.[595] In addition, each agency would contribute an equal share of the funding necessary for the sandbox framework's implementation.[596]

In the EU context, each Directorate General (DG) to which financial technologies are relevant could have the responsibilities of an agency as defined in the FSIA. The FSIO Liaison Committee could be a standing committee composed of representatives from the FSIOs of relevant DGs. Although each DG FSIO would abide by Section 3, the power to approve a petition could be raised to the standing committee. In this manner, the issue of a fintech's relevance to multiple agencies could be dealt with more efficiently and concertedly, thereby reducing the likelihood that a given compliance agreement developed for an approved petition might be subject to 'judicial review of another agency's or State's challenge to the agreement'.[597] The Liaison Committee could also involve representatives from ENISA, the ESAs' respective working groups / hubs on fintech innovation, and the ESRB.

The EU could extend ENISA's mandate for ENISA to advise each FSIO and the FSIO Liaison Committee. ENISA and the ESAs' fintech working groups / hubs could help each DG's FSIO to identify particular regulations that they would be willing to adjust in a sandboxing context, as per FSIA Section 3. ENISA and the ESAs could do so in cooperation with private-sector representatives, the Commission's FinTech Lab, and the ESRB.

Once a sandbox is up and running, the relevant ESA fintech working group / hub (with input from ENISA, relevant FSIOs with sectoral expertise, and the other ESAs' fintech working groups/ hubs) could communicate to a given fintech company which regulations apply, collect feedback from the company about the difficulties they encounter in attempting to comply, and advise the company on ways in which they might adjust their technology to comply with the necessary regulations and still pursue innovatory aims.

The company could potentially apply for consultations with the relevant ESA fintech working group/hub to discuss any particularly novel elements of a given emerging fintech before applying for a regulatory sandbox. Beginning such talks at an early stage and continuing them throughout

[594] The Financial Services Innovation Act of 2016 H.R. (114th Cong. 2016) 6118 Sec. 5, 6-7.
[595] ibid., Sec. 5, 8.
[596] ibid., Sec. 10, 17-18.
[597] ibid., Sec. 8, 14.

the R&D and sandboxing phases would reassure investors that a fintech is unlikely to have much regulatory pushback once it goes to market.

The ESAs' fintech working groups / hubs, the ESRB, and national supervisory authorities would be involved in supervising a fintech's integration into and effect on the financial system during and after the sandboxing period. They would also communicate with the Commission on possible systemic risks to which the fintech might give rise.

* * *

New technologies can operate on unprecedented paradigms. Prime examples are decentralised technologies like blockchain that have hardly any hierarchy and thus little distinction between controlling and processing parties. On the one hand, it is the responsibility of innovators to comply with established standards. On the other hand, our inability to foresee unprecedented technological paradigms means that regulations and standards that are developed for a particular technology landscape may contain elements that are not comprehensible in relation to relevant emerging technologies. Communication and cooperation between regulators and fintech companies are essential for lessening the disjunctions between law and emerging fintech and cultivating an innovation-friendly regulatory ecosystem. As indicated above, two recommended approaches are (1) more frequent evaluations of financial technologies and certifications/standards and (2) greater use of the regulatory sandboxing technique.

IV.V. SUGGESTIONS FOR BLOCKCHAIN

Since it looks probable that financial blockchains will be incorporated further into mainstream finance in the future,[598] it is important that consideration is given to security and regulatory issues that will become more pronounced if blockchain networks are scaled further. Furthering the development of shared blockchain cybersecurity standards and mechanisms that establish a strong unifying baseline for the many existing financial blockchains is crucial if banks are to achieve the high degree of interoperability required to operate initiatives such as blockchain-based interbank transfer systems.[599] This section considers how to further harmonise and facilitate oversight as well as the reporting and handling of incidents and vulnerabilities on financial blockchains. Finding ways of improving cooperation and consensus-building that can in turn improve the regulatory landscape and regulatory compliance, as well as oversight, reporting, and handling, is important if blockchains are to be further integrated into the financial system.[600]

This section therefore explores what a consortium for financial blockchains in the EU financial sector might look like: one that would enhance incident and vulnerability reporting and enable more effective blockchain governance and oversight. This section first assesses current EU blockchain harmonisation initiatives before assessing what an EU blockchain consortium might be able to learn from the development of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network, a successful financial messaging network of scale that has faced challenges analogous to those faced by decentralised fintech.[601]

i. Current EU Blockchain Harmonisation Initiatives

As outlined in Section III.V., significant progress has been made with the FATF Travel Rule, the 24 September 2020 proposals on Markets in Crypto-assets, and 'a pilot regime for market infrastructures based on distributed ledger technology'.[602] The former concerns the use of Virtual Asset Service Providers (VASPs) to identify the 'originator' and 'beneficiary' of cryptocurrency

[598] Kevin Werbach, *The Blockchain and the New Architecture of Trust* (MIT Press, 2018).
[599] Peter F. Cowhey, Jonathan D. Aronson: *Digital DNA: Disruption and the Challenges for Global Governance* (Oxford University Press, 2017) ch 7.
[600] Tom Lyons and Ludovic Courcelas, 'Blockchain and cybersecurity' (*EBOF,* 2020).
[601] Peter F. Cowhey, Jonathan D. Aronson: *Digital DNA: Disruption and the Challenges for Global Governance* (Oxford University Press, 2017) ch 7.
[602] FATF, '12-Month Review Of The Revised FATF Standards On Virtual Assets And Virtual Asset Service Providers' (FATF, 2020) <www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html> accessed 06 November 2020; Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and Amending Directive (EU) 2019/1937 COM(2020) 593 final; Proposal for a Regulation of the European Parliament and of the Council on a Pilot Regime for Market Infrastructures Based on Distributed Ledger Technology COM(2020) 594 final.

transfers.[603] The Markets in Crypto-assets proposal aims to strengthen and harmonise requirements for 'transparency and disclosure', 'authorisation and supervision', 'operation, organisation and governance', 'consumer protection rules', and 'measures to prevent market abuse'.[604]

In addition, the proposal for a regulation on 'a pilot regime for market infrastructures based on distributed ledger technology' would '[lay] down requirements on multilateral trading facilities and securities settlement systems using distributed ledger technology "DLT market infrastructures."'[605] These requirements regard '(a) granting and withdrawing ... specific permissions', '(b) granting, modifying and withdrawing related exemptions', '(c) mandating, modifying and withdrawing attached conditions, compensatory or corrective measures', '(d) operating such DLT market infrastructures', '(e) supervising such DLT market infrastructures', and '(f) cooperation between operators of DLT market infrastructures, competent authorities and ESMA'.[606] Incidents are reported to competent authorities and ESMA, and ESMA serves as a coordinator towards competent authorities on matters relating to distributed-ledger technologies (DLT), particularly supervision.[607] The proposal also involves an element of regulatory sandboxing in so far as one can apply for '[s]pecific permission to operate a DLT multilateral trading facility' and '[s]pecific permission to operate a DLT securities settlement system.'[608] All these measures contribute to the harmonisation of the blockchain landscape.

This paper considers how recent regulations might be reinforced through a consortium approach towards governance and oversight for blockchains in the EU. This paper promotes the establishment of a consortium/entity that brings the various decentralised financial technologies together to liaise with EU authorities, strengthen the reporting and handling of mechanisms, and mitigate regulatory issues (particularly issues relating to the identification of hierarchies of responsibility on decentralised fintech that are not resolved by the recent proposals).

[603] FATF, '12-Month Review of The Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers' (FATF, 2020) <www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html> accessed 06 November 2020.
[604] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and Amending Directive (EU) 2019/1937 COM (2020) 593 final Title I Art. 1.
[605] Proposal for a Regulation of the European Parliament and of the Council on a Pilot Regime for Market Infrastructures Based on Distributed Ledger Technology COM (2020) 594 final Art. 1.
[606] ibid.,
[607] ibid, Art. 9.
[608] ibid, Art. 4, 5, 7, 8.

There are several blockchain-related EU initiatives, besides the 24 September proposals, that have made strides in researching and addressing various issues related to the integration of blockchains with the wider EU economy.[609] Based on the insights gathered and gaps identified in the following survey of key initiatives, this section puts forward the idea of a softly-centralised governance and oversight consortium/entity that can reinforce the recent regulation proposals and existing initiatives.

EBSI Initiatives

In April 2018, the European Commission established the European Blockchain Services Infrastructure (EBSI) in conjunction with the member states. The aim of EBSI is the development and delivery of public services to the citizens of EU member states. EBSI aspires to create public services that are interoperable (with each other and among the member states), are in full compliance with EU law, and uphold the principles of security, data privacy, and energy efficiency to their highest standards. Part of EBSI's mission is to develop specifications regarding software reusability and to help EU institutions and the private sector to adopt blockchain-based solutions.[610]

INATBA Initiatives

The Brussels-based International Association for Trusted Blockchain Applications (INATBA), established in April 2019, has recognised the need to develop a common blockchain standard to unify the wide range of blockchain technologies that currently exist.[611] INATBA's initiatives significantly help to promote and delineate blockchain uptake through appropriate regulatory foresight. INATBA aims to use public-private cooperation to promote better use and regulation of blockchain. It brings together blockchain suppliers and users with representatives of governmental and standard-setting bodies from across the world. INATBA develops guidance on governance with respect to various blockchain technologies.[612] Its guidance on governance looks to take into account 'economic, social, legal and technical considerations'.[613] In response to

[609] Tom Lyons, Ludovic Courcelas, and Ken Timsit, 'Blockchain and the GDPR' (The EU Blockchain Observatory and Forum, 2018).
[610] 'The European Blockchain Services Infrastructure is on its Way' (*CEF Digital*, 25 September 2019) <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/09/25/The+European+Blockchain+Services+Infrastructure+is+on+its+way> accessed 06 October 2020.
[611] 'Blockchain Technologies' (*European Commission*, 2020) <https://ec.europa.eu/digital-single-market/en/blockchain-technologies> accessed 7 March 2020.
[612] 'Governance Working Group' (*INATBA*) <https://inatba.org/working-groups/governance-working-group/> accessed 20 December 2020.
[613] ibid.

the Commission's recently proposed regulation for Markets in Crypto-Assets (MICA), INATBA established a MICA task force to liaise with regulators with respect to this regulation.[614]

B-Hub for Europe

B-Hub for Europe looks to facilitate scalability and interoperability as well as an improved regulatory landscape for blockchain start-ups across a range of sectors. The initiative is focused on helping five blockchain start-up ecosystems (in Italy, Germany, France, Lithuania, and Romania) to communicate, integrate, and scale with one another such that '[p]ublic and private actors involved will benefit from a tailormade knowledge transfer process on blockchain technologies and use cases for internal barriers removal and faster adoption.'[615] In particular, its mission is to foster the '[m]apping of technology excellence in the blockchain field', '[s]tronger and more connected blockchain communities', '[n]ew market channels ... for blockchain startups', '[m]ore motivated and engaged demand from the public and private sector', '[e]mpowered startups with business and market skills to scale into the EU and international market', and 'links and cooperation between startups and public/private potential customers/users'.[616] In addition, it liaises with regulators 'to improve the regulatory context at EU level'.[617] B-Hub benefits from the EU's Horizon 2020 Research and Innovation programme.[618] The project started on 1 January 2020 and extends through 2021.[619]

EBOF Reports

The European Blockchain Observatory and Forum (EBOF) is a European Parliament pilot project. It is a tool for the EU to test new policy initiatives and prepare for future measures.[620] The EBOF analyses and reports on a range of areas relating to blockchain and offers insights and recommendations about how the EU can protect consumers while supporting blockchain-related innovation.[621] This section touches on many of the aspects that the EBOF has considered in its various reports. These include the relationship of blockchain, governance, scalability, and cybersecurity.

---

[614] 'INATBA MiCA Task Force' (*INATBA*) <https://inatba.org/mica-task-force/> accessed 27 December.
[615] 'Blockchain HUB FOR EUROPEan Startups Acceleration and Growth' (*European Commission: CORDIS EU research results*, 3 July 2020) <https://cordis.europa.eu/project/id/871869> accessed 27 December 2020.
[616] 'About' (*B-hub: Blockchain for Europe*) <https://b-hub.eu/about/> accessed 27 December 2020.
[617] ibid.
[618] 'Blockchain HUB FOR EUROPEan Startups Acceleration and Growth' (*European Commission: CORDIS EU research results*, 3 July 2020) <https://cordis.europa.eu/project/id/871869> accessed 27 December 2020.
[619] ibid.
[620] 'Reports' (*EBOF*) <www.eublockchainforum.eu/reports> accessed 22 February 2020.
[621] 'About' (*EBOF*) <www.eublockchainforum.eu/about> accessed 06 October 2020.

The EBOF's projects and initiatives are relatively recent developments. As such, they are in their exploratory phases, trying to answer numerous questions related to blockchain's legal compliance and its wider integration into the EU's financial system. The EBOF acknowledges that a degree of abstraction within their recommendations is currently unavoidable.[622] The EBOF's recommendations at this stage are less frameworks for particular use cases or sectors than calls for more attention to, and future work on, particular issues.[623]

The EBOF's research has thus sought to pinpoint problem areas that require greater attention. In doing so, it has outlined several key characteristics and principles that should be considered when developing consortia or a 'European Blockchain Infrastructure'.[624] The EBOF notes that prioritising scalability and security negatively impacts decentralisation.[625] Prioritising scalability and decentralisation also negatively impacts decentralisation whilst prioritising security and decentralisation negatively impacts scalability.

In its report on scalability, interoperability, and sustainability, the EBOF recommends that the EU should focus to a greater extent on standards development.[626] The report also highlights the need to further facilitate relevant research and handle legal grey-zones.[627] Though it points to the need for more research with respect to governance, the report suggests that a given set of live blockchains are best governed by a consortium of stakeholders, and that governance is likely to be most effective on a sectoral or use-case basis.[628] It also emphasises the need for clear membership rules.[629] In addition, it recommends that 'the EU take a wait-and-see approach, giving projects the time to experiment and learn before developing standards or considering governance related regulations.' In this latter respect, regulatory sandboxing is relevant.

In addition, the EBOF advocates 'ecosystem diversity', by which it means a multiplicity of blockchain technologies within an overarching European Blockchain Infrastructure.[630] It

[622] Tom Lyons and Ludovic Courcelas, 'Governance of and with Blockchains' (*EBOF*, 2020) 27.
[623] Ludovic Courcelas, Tom Lyons, and Ken Timsit, 'The EU Blockchain Observatory and Forum, Conclusions and Reflections 2018-2020 (*EBOF*, 2020) 20-21.
[624] These include 'technological diversity', 'interoperable communications', 'strong digital identity', 'fiat currency payments', sever and data backups, 'roll-back functionalities', and 'migration / living wills' for transferring data out of a platform. Tom Lyons, Ludovic Courcelas, and Ken Timsit, 'Scalability, Interoperability, and Sustainability of Blockchains (*EBOF*, 2019)17-18.
[625] ibid., 10-11.
[626] ibid., 20-21.
[627] ibid.
[628] ibid., 7-8, 20-21.
[629] ibid., 14.
[630] ibid., 20-21.

highlights diversity's benefits for innovation.[631] In addition, it notes that such diversity will prevent 'vendor lock-in' and prompt greater attention to interoperability.[632] As an aspect of this diversity, the report also argues that 'policy makers should encourage fiat money on-chain to facilitate blockchain-based payments and the uptake of smart contracts'.[633] The report's recommendations conclude with an exhortation to policy makers to be attentive to blockchain developments, to attend to grey-zones in legal frameworks vis-à-vis blockchain, and to promote and facilitate education about decentralised technologies.[634]

The EBOF's paper on governance voices similar themes, with an additional emphasis on the need to 'collect and communicate best practice.'[635] It outlines various types of blockchain governance and specifies what should motivate the formation of a blockchain consortium.[636] The report notes that 'blockchain consortia tend to be born of shared business problems'.[637] In the context of this paper and the issues outlined earlier, the shared problems concern financial cybersecurity and blockchain's relationship with existing regulations.

ii. Developing a Governance and Oversight Entity for Financial Blockchains

Whereas INATBA, B-Hub, and the EBOF handle decentralised technologies in a broader sense, the following discussion focuses on blockchain financial technologies in an EU context and considers how they might be better governed and maintained in the interest of financial cybersecurity. In doing so, this discussion builds on the EBOF's research regarding the status and development of blockchain-related governance, scalability, and sustainability. This discussion aims to outline a more concrete framework for governance and oversight for the EU's financial blockchain ecosystem. At the same time, it is constrained by some of the same factors that require the EBOF's recommendations to remain abstract at this time.

B-Hub is already making strides to facilitate cooperation, scalability, interoperability, innovation, and regulatory improvement across five blockchain ecosystems and offers a forum of cooperation from which the suggested governance and oversight entity might be pursued. However, B-Hub does not constitute a consortium for the EU's financial blockchain ecosystem

[631] Tom Lyons, Ludovic Courcelas, and Ken Timsit, 'Scalability, Interoperability, and Sustainability of Blockchains (*EBOF*, 2019) 21.
[632] ibid., 17.
[633] ibid., 21.
[634] ibid., 20-21.
[635] Tom Lyons and Ludovic Courcelas, 'Governance of and with Blockchains' (EBOF, 2020) 27.
[636] ibid., 1-34.
[637] ibid., 17.

that comes together to make decisions on matters of ecosystem governance, oversight, incident reporting, incident handling, and accountability detection.

This paper thus outlines a softly-centralised entity/consortium involved in cybersecurity, standardisation, reporting, and oversight with respect to financial blockchains. Such an entity might cooperate closely with a cyber hub (e.g., the variants discussed in Section IV.I.). The issues of governance and oversight in relation to better cybersecurity, incident detection, incident reporting, and incident handling are central to the following discussion.

The following sub-sections look at use cases and existing blockchain-based solutions, as well as comparisons between blockchain-based solutions and non-blockchain-based solutions. They recommend a softly-centralised governance model with an EU-wide scope. In other words, the suggested governance and oversight entity is a sectoral consortium for stakeholders of financial blockchains in the EU context. Building on the EBOF's emphasis on maintaining the 'ecosystem diversity' of blockchain technologies,[638] it should be seen as a consortium of stakeholders involved in the various financial blockchain technologies that connect across the EU. Such a consortium could be a steppingstone to one at an extra-European level.

This paper's suggestions for a soft-centralisation model for blockchain governance, inspired in part by SWIFT, can be considered complementary to the insights gathered by the EBOF in their reports and as a more detailed extension of the EBOF's proposals on blockchain governance and scalability. The insights presented throughout this section can help to achieve the European Commission and EBOF's vision of a cybersecure and consolidated European Digital Single Market where blockchain can play an integral role. Establishing a softly-centralised governance and oversight entity for blockchain-based financial networks could reinforce the Commission's proposed regulation on 'a pilot regime for market infrastructures based on distributed ledger technology' by helping to further harmonise regulatory oversight and strengthen the reporting environment. In cooperation with initiatives like INATBA and B-Hub, the suggested entity would also facilitate the sustainability, scalability, and interoperability of blockchains in the EU's financial system. This paper's suggested implementation for the EBOF's idea of a consortium of stakeholders includes the competency to propose and democratically settle on common standards in complement to EU regulations and to detect and handle blockchain-based cyber

[638] Tom Lyons, Ludovic Courcelas, and Ken Timsit, 'Scalability, Interoperability, and Sustainability of Blockchains (*EBOF*, 2019) 20-21.

incidents. The softly-centralised entity suggested in this section would serve as a standard-making, consensus building, report-facilitating, and oversight entity for financial blockchains in the EU.

The Dangers of Over-Centralisation

Before exploring soft-centralisation further, it is important to first consider the dangers of over-centralising. Many of the cryptocurrency (or virtual asset) networks seek to follow the purist decentralisation approach as much as possible. This is an approach that is strongly adhered to by Bitcoin (the most influential of all cryptocurrencies). A permissionless blockchain is a blockchain that is predicated on the idea of pure decentralisation, according to which no node has authority over another. A fully-decentralised system is trustless because it does not rely on intermediaries. This contrasts with a permissioned blockchain, which requires layers of 'permissions' for its various operations. Attempts to pursue more centralised decision-making on highly decentralised blockchains come with the risk of hardforks and chain splits, by which parts of the main network break off to form their own network(s).

Blockchain hardforks are usually a result of a difference in community opinion related to underlying blockchain protocol. This often leads to a split in the community and, eventually, to one in the underlying blockchain platform as well. The most prominent examples of hardforks or chain splits are those of Bitcoin Cash (the result of a difference in community opinion related to underlying Bitcoin protocol) and Ethereum Classic, which broke from the main Bitcoin and Ethereum networks respectively (see Appendix v for more on the Ethereum split).[639] This shows that even these major networks could not keep the whole community intact when some members of these communities tried to deviate from the notion of pure decentralisation.

Given these risks, one must be cautious about the degree of centralisation to pursue. As much as there are benefits to blockchain networks that are not purely decentralised—chiefly security and scalability[640]—the risk of splits increases the more an effort is made to centralise networks that value a degree of decentralisation. An international organisation that seeks to bring multiple

[639] George Donnelle 'A Manifesto for the Next 10 Years of Bitcoin (Cash, September 2020)' <https://read.cash/@georgedonnelly/a-manifesto-for-the-next-10-years-of-bitcoin-cash-c67d115a > accessed 08 October 2020; 'Bitcoincash' (*BitcoinCash*) <https://www.bitcoincash.org/faq/ > accessed 08 October 2020; 'A Crypto-Decentralist Manifesto' (*Ethereum Classic*, 11 July 2016) <https://ethereumclassic.org/blog/2016-07-11-crypto-decentralist-manifesto> accessed 08 October 2020.
[640] Tom Lyons, Ludovic Courcelas, and Ken Timsit, 'Scalability, Interoperability, and Sustainability of Blockchains (*EBOF*, 2019) 10-11.

blockchain networks into a governance framework needs to also consider that governance issues tend to amplify the more governance is scaled.

Soft-Centralisation

A softly-centralised approach would help to reduce fragmentation while at the same time reducing the likelihood of potential splits within a given blockchain network. The following sub-sections therefore recommend a consortium (in the form of a softly-centralised entity partly inspired by SWIFT's governance model) with goals including the improvement of common standards, incident detection, and reporting. With respect to soft-centralisation, this paper draws on the approach that the EBOF describes as '[collective governance]', such as by on-chain stakeholders with input from off-chain stakeholders.[641] Although it can be challenging to reconcile an overarching entity/consortium with blockchain's decentralised nature and principles, the SWIFT network, the EBOF's consortium suggestions, Opensource Software Management, and Bitcoin Improvement Proposals offer inspiration for potentially viable soft-centralisation.

Consortium governance could take the form of a 'multi-stakeholder-managed industry consortium', a 'single stakeholder-managed, blockchain-based industry ecosystem', or a 'geographically based blockchain [consortium]'.[642] The EBOF describes the former as one 'governed collectively' by multiple stakeholders. The single stakeholder model is one in which 'a single provider may build a platform and open it up for others to use'. A geographically-oriented model would be 'a general purpose, large-scale platform for more or less general transacting entities within a defined community that provides an infrastructure for members to build upon'. Given this paper's sectoral and geographic focus, it explores governance mainly in relation to the 'multi-stakeholder-managed industry consortium'. At the same time, it incorporates some characteristics of a more geographically-oriented consortium.

Opensource Software (OSS) management would be an important element of soft-centralisation.[643] Subsequent sub-sections thus touch on the Linux Foundation with respect to distributing the membership for this entity. By facilitating communication between two or more distinct blockchain platforms, the suggested entity would provide a forum for different

[641] Tom Lyons and Ludovic Courcelas, 'Governance of and with Blockchains' (EBOF, 2020) 14; Tom Lyons, Ludovic Courcelas, and Ken Timsit, 'Scalability, Interoperability, and Sustainability of Blockchains (*EBOF*, 2019) 8 (qu.).
[642] Tom Lyons, Ludovic Courcelas, and Ken Timsit, 'Scalability, Interoperability, and Sustainability of Blockchains (*EBOF*, 2019) 8.
[643] Rowan van Pelt, et al., 'Defining Blockchain Governance: A Framework for Analysis and Comparison', (Information Systems Management, 2020) 5.

opensource blockchain platforms to come together to solve issues surrounding blockchain interoperability. In doing so, the entity would facilitate the scalability and proliferation of blockchain networks.

The suggested entity could also use community-driven Bitcoin Improvement Proposals (BIP) as a model for developing common standards for blockchain protocols. Using a similar approach in relation to a broader community of financial blockchains to develop shared baseline standards would reduce fragmentation in the way individual blockchain projects are developed and operated. Complementing efforts to improve standards through regulation, such as mechanisms that strengthen baseline standards for blockchains throughout the EU, would make it easier for companies and individuals to adopt blockchain for their projects. In addition, such standardised protocols would allow relevant entities to oversee and regulate blockchains more effectively.

The SWIFT, OSS, and BIP comparisons are discussed further in following sub-sections.

Place in the EU Ecosystem

The softly-centralised entity would ideally encompass financial blockchain networks across the EU and facilitate the proliferation and maintenance of an EU-wide financial gross settlement system. This entity could forge close ties with an EU-level cyber hub (see Section IV.I.), regulators, and other authorities in relevant jurisdictions. It would be in close contact with regional/local competent authorities and law enforcement offices that handle incident reporting and identify responsible parties. The softly-centralised entity would facilitate reporting to the cyber hub and the cyber hub would then work with the entity and law enforcement offices to handle incidents and vulnerabilities.

Public-sector stakeholders could thus include competent authorities and other relevant EU bodies/initiatives (e.g., the Commission, ENISA, the EBA, the ESMA, the ECB, a potential cyber hub, national central banks, national governments, and other relevant competent authorities) with whom the private sector stakeholders would liaise. Other stakeholders would include initiatives like INATBA and B-Hub. Figure 1, outlined at the end of this section, provides an overview of how the suggested entity would link public, technological, and corporate stakeholders.

The presence of SWIFT and of many EU blockchain-based initiatives in Brussels can facilitate the establishment of such an entity for blockchain. This proximity of relevant entities should be utilised to cross-pollinize ideas and expertise. As was the case with SWIFT, it would be in the

EU's interest to promote and facilitate the establishment of such an entity for blockchain as it would further strengthen the Digital Single Market.

Not a Commercial Competitor

It is worth clarifying here that this paper's proposed entity would not be a commercial competitor in the wider blockchain space. Rather, it would act as a management layer for fostering communication, consensus, cooperation, and order among its on-chain stakeholders (i.e., blockchain members) in consultation and cooperation with off-chain stakeholders. In doing so, it would facilitate standardisation as well as cyber incident detection and reporting. The entity/consortium members could work together on the development and adoption of tools for monitoring data and financial flows through blockchain networks to detect anomalies. In addition to detecting incidents or suspicious behaviours as they occur, the tools would facilitate incident pre-emption by raising a flag in light of suspicious activity/anomalies. These methods might utilise intelligent techniques, such as machine learning, to make decisions with reference to the underlying system's execution history.

This section consequently focuses on establishing a softly-centralised entity/hub/consortium for governance and oversight, as opposed to an entity that commercially offers a connecting platform or other product or service. In cooperation with initiatives like B-Hub and INATBA, the suggested entity would act as a hub for the peers of the open-source blockchain community, the crypto-corporate sector (such as exchanges, custodians of virtual assets, and VASPs), government institutions, and law enforcement entities. The suggested entity can be considered an information portal, a standard-making and consensus-building consortium, as well as a facilitator and coordinator for blockchain incident detection and reporting (see Figure 1). It would be the blockchain partner to a wider cyber hub, with which it would work in close cooperation.

The Maturation of Soft-Centralisation

As mentioned previously, blockchain and all the other products it has inspired are still in their early stages. As much as these technologies are growing, it will take some time before these systems find their place in the mainstream financial industry. Robleh Ali discusses this aspect in his study concerning designs for a digital fiat cryptocurrency.[644] Ali notes that most technological innovation requires organisational innovation.[645] Without the corresponding organisational

[644] Robleh Ali. 'Cellular Structure for a Digital Fiat Currency.' (*P2P Financial System International Workshop, Federal Reserve Bank of Cleveland*, 2018) 27.
[645] ibid.

innovation, a technological innovation's full potential cannot be tapped. For example, although the financial industry became digitalised as soon as the first computer network was used for financial messaging it was only after relevant people became savvy about personal computing and digital correspondence that it fully took off.[646] SWIFT took some time to gain traction in its early stages for similar reasons. Comparably, our suggested softly-centralised entity for blockchain governance would require an innovative organisational mindset for full implementation. As a softly-centralised 'bystander' organisation, the entity would deemphasise conventional (i.e., centralised and top-down) organisational power. This would be in part because of a shift in balance from human-based trust to technology-based trust. It will be when more people have a good understanding of blockchain technology, and when there are applications with better and more user-friendly interfaces, that blockchain (and the suggested entity) will truly 'take off.'

Blockchain in its early stages is going through something similar to what the Internet went through in its early stages. Rather than being a commercial product of any one business, the Internet's development was founded on its users' community efforts. What this paperproposes is a platform for all flavours of blockchains (i.e., permissioned or permissionless) to come together and converge in terms of interoperability, scalability, and adaptability. The presence of such a platform would help to bring distinct factions of the blockchain community together, as SWIFT did with banks in the 1970s.[647] It would help to build greater context and formality for the blockchain community so that it can pursue consensus on issues surrounding governance, incident reporting, incident handling, interoperability, scalability, and management.

iii. SWIFT and Blockchains

There is much to be learnt from SWIFT's development in terms of best practices for establishing soft-centralisation. The development of the entity suggested in this section can be seen as a process similar to what SWIFT went through in its early stages when it proposed an alternative to financial services' status quo. The following sub-sections look at what can be learnt from SWIFT's soft-centralisation approach towards its stakeholders, as well as at what approaches might be needed to connect blockchains on a scale comparable to SWIFT's.

[646] Robleh Ali. 'Cellular Structure for a Digital Fiat Currency.' (*P2P Financial System International Workshop, Federal Reserve Bank of Cleveland*, 2018) 27.
[647] ibid.

SWIFT was created in 1973 to facilitate a high volume of international financial transactions.[648] Like blockchain, SWIFT uses computer networking to offer secure financial messaging among financial institutions and to thereby facilitate financial transactions among these entities.[649] There has been some debate about the extent to which decentralised fintech like blockchain will displace SWIFT as cross-border payment platforms, and it remains to be seen what the relationship of SWIFT and blockchain fintech will turn out to be.[650]

SWIFT has also begun to experiment with its own blockchain capabilities, and it has been suggested that it could facilitate blockchain interoperability.[651] In a 2019 interview, Lisa O'Connor, SWIFT's Managing Director for Standards and Capital Markets for the Asia-Pacific, indicated that SWIFT could possibly serve as a connecting hub for a largescale blockchain network.[652] As such, it would be 'a platform that helps to connect our members up to the best of these blockchain solutions'.[653] SWIFT indicates in a position paper on its relationship with distributed ledger technologies that it considers itself uniquely positioned to connect and develop 'industry standard DLTs' at an international scale that are subject to good governance, meet high security standards, and comply with national and international regulations.[654] SWIFT has primarily expressed an intention to develop blockchain interoperability and governance for financial messaging specifically, as opposed toserving as a governance authority and connecting platform for financial blockchains more generally.

iv. Solving Fragmentation Through Soft-Centralisation

Much like blockchain, SWIFT is primarily a service infrastructure with an overall aim of enabling fast, economical, and secure communication among its members. SWIFT is an overarching non-profit with a main office near Brussels that facilitates cooperative decision-making and

[648] Peter F. Cowhey, Jonathan D. Aronson, *Digital DNA: Disruption and the Challenges for Global Governance* (Oxford University Press, 2017) ch 7.
[649] ibid.
[650] Frances Coppola, SWIFT's Battle for International Payments. (*Forbes*, 16 July 2019) https://www.forbes.com/sites/francescoppola/2019/07/16/swifts-battle-for-international-payments/#1162a9dc758e accessed 30 September 2020; Chris Skinner, 'Will the Blockchain Replace Swift?' (*American Banker*, 8 March 2016) <www.americanbanker.com/opinion/will-the-blockchain-replace-swift> accessed 30 September 2020.
[651] Can SWIFT Help with Blockchain Interoperability? (Ledger Insights) <www.ledgerinsights.com/can-swift-help-with-blockchain-interoperability/> accessed 1 October 2020; 'SWIFT talks about XRP – Hong Kong Blockchain Week!' (*CNBC Africa*, 11 March 2019) <https://youtu.be/xS36_foCEQ4?t=863> accessed 30 September 2020.
[652] 'SWIFT talks about XRP – Hong Kong Blockchain Week!' (*CNBC Africa*, 11 March 2019) <https://youtu.be/xS36_foCEQ4?t=863> accessed 30 September 2020.
[653] ibid.
[654] 'SWIFT on Distributed Ledger Technologies: Delivering an Industry-Standard Platform through Community Collaboration' (*SWIFT* & *Accenture* 2016) 16-17.

standardisation with respect to the protocols that govern SWIFT's operations.[655] SWIFT strives for international regulatory harmonisation through soft-centralisation.[656]

SWIFT thus offers a model for soft-centralisation (i.e., an overarching, non-profit, and neutral organisation in charge of underlying financial network maintenance). Such soft-centralisation allows international actors across the public and private sectors to come together to form a decision-making entity. As part of this, SWIFT gives overview access to relevant government institutions.[657] Each year, members of G10 central banks review SWIFT's network and its operations. SWIFT has thus been able to foster a productive private-public relationship.[658]

An analogous entity could be developed for blockchain platforms that would facilitate close cooperation with public entities/stakeholders and could foster efficient cyber incident detection and reporting. Such an entity would be in contact with relevant European entities (e.g., the Commission, ENISA, the EBA, the ESMA, the ECB, national central banks, a potential cyber hub, national governments, and other relevant competent authorities) to keep pace with EU-wide regulations and financial processes. Such an entity would also work closely with initiatives including INATBA and B-Hub.

Though parallels are being drawn between SWIFT and this paper's suggested entity, the latter's relationship with banks would not be the same as SWIFT's. SWIFT provides a specific service for and is cooperatively owned by banks / mainstream financial institutions, whereas the suggested entity would liaise with the mainstream financial system on matters of governance and standardisation as well as incident reporting and handling processes. While some of the entity's on-chain members might be financial blockchains developed by banks, its members would not primarily be mainstream financial institutions.

In order to foster a more standardised environment, this entity would need to forge close ties with individual regulators and jurisdictions. A potential model might be the UN's framework for creating jurisdiction-specific Financial Intelligence Units (FIU), which are mainly responsible for

[655] 'Organisation & Governance' (*SWIFT*) <https://www.swift.com/about-us/organisation-governance> accessed 08 October 2020; Peter F. Cowhey, Jonathan D. Aronson, *Digital DNA: Disruption and the Challenges for Global Governance* (Oxford University Press, 2017) ch 7.
[656] Peter F. Cowhey, Jonathan D. Aronson, *Digital DNA: Disruption and the Challenges for Global Governance* (Oxford University Press, 2017) ch 7.
[657] ibid.
[658] ibid.

implementing Anti Money Laundering operations in a local area.[659] A similar framework could be envisioned for the implementation of blockchain standards in general and AML regulations in particular. Such a framework could further improve blockchain's proliferation by enabling more businesses to adopt this technology without themselves needing to worry extensively about some of the fine details of regulatory compliance. Building on and reinforcing INATBA and B-Hub's work, the entity could also work closely with regulators in an advisory role to encourage the formation of regulatory frameworks that are flexible and implementable towards emerging financial use cases of blockchain.

SWIFT grants full membership rights to entities that are well-governed according to their local laws and common SWIFT standards and have reached a certain share of the network's transaction volume. Smaller financial institutions that do not have the requisite transaction volume can take part in the network through full members (i.e., through a tiered system where larger financial institutions can encompass smaller ones and represent them in SWIFT's network).[660] An issue that can arise is that the larger full members might dominate decision-making and might impose unwarranted sanctions on rival financial institutions that do not have the same amount of influence on the network (e.g., through restricting their access to the network).[661] SWIFT tries to address this integrity issue by holding an annual external audit of the system and by regularly re-evaluating membership when a member's market shares change.[662]

Blockchain's inherent tamper-evident record keeping and transaction transparency would help to mitigate various integrity issues for an analogous softly-centralised entity for blockchain.[663]

v. Overcoming Challenges for Soft-Centralisation

The creation of a softly-centralised entity for blockchain is likely to be challenging, especially when it comes to the issue of membership. Its governance challenges, and its challenge of still being largely an alternative financial service to the existing status quo, are likely to be similar to those that SWIFT has experienced. Unlike SWIFT, however, membership cannot simply be determined based on transaction volume due to blockchain's decentralisation and anonymity principles. Due to these features, as well as to regulations like KYC and AML, it becomes

[659] 'United Nations Convention Against Transnational Organized Crime and The Protocols Thereto' (*United Nations: Office on Drugs and Crime*, 2004)
[660] Peter F. Cowhey, Jonathan D. Aronson, *Digital DNA: Disruption and the Challenges for Global Governance* (Oxford University Press, 2017) ch 7.
[661] ibid.
[662] ibid.
[663] ibid.

challenging for an overarching entity for blockchain to distribute membership while still being in compliance with legal frameworks. The problem is particularly manifested in permission-less systems such as Bitcoin and other cryptocurrency networks where it is difficult to establish the real identity of a participating node. In general, it is difficult (and usually goes against a public blockchain's anonymisation principle) to identify whether an entity is an institution or an individual, or even an automated bot.

However, an umbrella non-profit entity such as the Linux Foundation could serve as a membership model for taking an opensource software management approach towards many of the participating blockchain platforms.[664] The Linux Foundation maintains and standardises the open-source codebase for many of its projects. The companies, individuals, and entities who use and deploy these software products can be part of this foundation depending upon their reputation for compliance with their local regulations. Each member helps to maintain and standardise the open-source code. This model fits the open-source nature of many blockchain-based platforms.

Furthermore, a system akin to Bitcoin Improvement Proposals (BIP) could be adopted and formalized.[665] Doing so would create a standardisation mechanism for the protocols that govern the underlying technology of many of the blockchain-based projects. BIPs are community-driven improvement suggestions.

vi. Complementing Reliability and Efficiency with Cybersecurity

Most financial systems often put more emphasis on reliability and efficiency than cybersecurity. Confidentiality, integrity, reliability, and transparency are usually deemed the most important factors for designing a new financial service solution.[666] SWIFT first focused on these aspects and later started to incorporate cybersecurity measures. Fortunately for blockchain, these reliability and efficiency aspects are to a large extent inherent to the way blockchain operates.[667] In order to incorporate the (cyber)security aspects further, particularly in the light of increasing integration

[664] Linux Foundation, 'Join the Linux Foundation' (*Linux Foundation*) <www.linuxfoundation.org/membership/join/> accessed 08 October 2020; Rowan van Pelt, et al. 'Defining Blockchain Governance: A Framework for Analysis and Comparison', (Information Systems Management, 2020) 5.
[665] 'Bitcoin Improvement Proposals' (*Github*) <https://github.com/bitcoin/bips > accessed 08 October 2020.
[666] Peter F. Cowhey, Jonathan D. Aronson, *Digital DNA: Disruption and the Challenges for Global Governance* (Oxford University Press, 2017) ch 7.
[667] Mike Orcutt, 'How Secure is Blockchain Really?' (*MIT Technology Review*, 2018) <https://www.technologyreview.com/2018/04/25/143246/how-secure-is-blockchain-really/> accessed 08 October 2020.

with the mainstream financial market, there needs to be a mechanism that can detect incidents and attribute accountability to different entities across the system.

In systems like SWIFT and blockchain, the cybersecurity issues are usually international, such that reporting and accountability mechanisms need to be considered in relation to cross-national cybersecurity and data protection regulations. Blockchain's decentralised nature and its anonymity principle make cross-border incident detection and accountability attribution particularly difficult.[668] As discussed in Section III.V., tensions between blockchain and regulations have an impact on the feasibility of reporting and handling incidents that occur on blockchain technologies.

vii. Summary of Blockchain Governance Suggestions

As integration with, or replacement of, existing financial systems rises, the establishment of a softly-centralised governance and oversight entity/consortium for financial blockchains operating in the EU would help to reinforce financial cybersecurity by harmonising standards and facilitating more concerted incident detection, investigation, reporting, and handling. This entity would facilitate the proliferation and maintenance of the EU blockchain ecosystem as a whole and would form standards that govern the technical operations of the underlying systems. Given its international perspective, a softly-centralised governance and oversight entity for blockchain that works closely with a more general EU-level cyber hub and relevant EU entities would be well-placed to issue guidance on the responsibility of actors in a decentralised system. Such an entity would also aim to strike a balance between respecting blockchain's core principles (i.e., tamper-evident public record keeping, anonymity, and distributed consensus) and compliance with existing legal frameworks (e.g., GDPR, KYC, and AML). This would be facilitated if membership within this softly-centralised entity were to be based on respect for impartiality, the rule of law, open-source technology, and an appropriate distribution of power.

This entity would work with public authorities on these issues. It would be in contact with the Commission, ENISA, the EBA, the ESMA, the ECB, national central banks, INATBA, a potential cyber hub, national governments, and other relevant competent authorities (see Figure 1). Such cooperation would help this entity to keep pace with regulations and financial processes and to develop appropriate stress tests within EU jurisdictions. The entity would provide information and analysis on cross-border incidents to these authorities where relevant.

[668] Tom Lyons, Ludovic Courcelas, and Ken Timsit, 'Blockchain and the GDPR' (*EBOF*, 2018).

Given the scope of this paper and the practicalities of implementation, the suggested framework is directed at the EU's financial sector and proposed in relation to EU bodies. However, such a framework at the EU-level could serve as a steppingstone to one that draws stakeholders from across the global financial system.

To conclude, there are four main benefits to establishing a softly-centralised governance and oversight entity for financial blockchain networks.

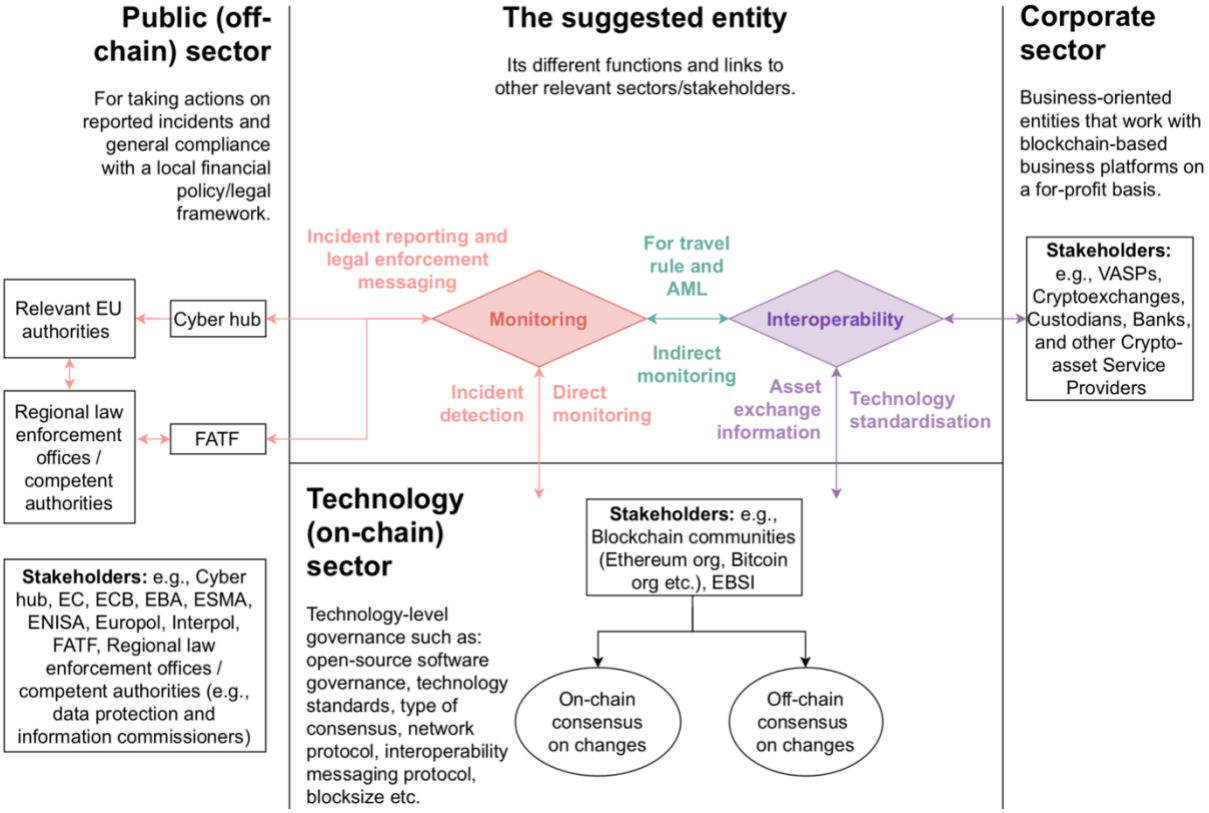
- First, such an entity would facilitate compliance with, and consensus about, national and international legal frameworks by bringing financial blockchain platforms into closer communication and by working closely with the ESMA, ENISA, competent authorities, and the Commission.

- Second, soft-centralisation would help to pre-empt and mitigate the risk of undemocratic hardforks or chain splits, which occur when a faction splits from a blockchain network (see Ethereum Classic and Bitcoin cash splits in Appendix v). Such events tend to be somewhat political in nature rather than purely technical. Soft-centralisation would help the community to come together out of their own initiative to discuss and solve issues. In doing so, it would help to reduce the likelihood of such splits.

- Third, such an organisation would improve incident detection and reporting for blockchain-based cybersecurity incidents by facilitating an overview of the network and making more a concerted allocation of responsibility possible. It could set up regional offices that could play a role in reporting incidents and could work closely with a potential cyber hub.

- Fourth, soft-centralisation for the blockchain space makes it more difficult for a region or entity to monopolise the blockchain system. One issue is that dominating blockchain mining hubs can emerge in various geographic locations as a result of a relatively large and (often) intentional accumulation of computational resources. These hubs can undermine the decentralised character of blockchain systems (e.g., see Appendix vi). With the presence of an overarching organisation that has a fair and democratic membership system, such monopolies might be kept in check.

Figure 1: Outline of stakeholder relationships



IV.VI. IMPROVING INSURANCE FOR CYBER WAR/TERRORISM

The following discussion first considers existing initiatives for improving coverage for cyber war and cyber terrorism. It then puts forward further suggestions for improving the financial sector's resilience against such events. Pre-empting and mitigating the financial repercussions of such incidents are an important component of a holistic financial cybersecurity approach that takes into account market confidence and the possibility of cyber-induced systemic instability.

This paper suggests,

- An EU commercial cyber risk pool (composed of private-sector institutions) that would offset the European financial system's cyber risk, which is currently exacerbated by cyber war/terrorism exclusion clauses. This pool would offer explicit coverage for acts of cyber war/terrorism. It would also have a rapid response mechanism for covering infrastructural and operational costs of combatting and recovering from a large-scale cyberattack.

i. The Commission's Initiative for an EU Cyber Emergency Fund

An initiative that is already being considered by the Commission that could mitigate cyber warfare and any cyber-induced systemic instability is an EU Cyber Emergency Fund. This fund could fill gaps left by omissions in, or the absence of, national terrorism risk insurance programmes. According to the definition provided in the Commission's 2017 Impact Assessment regarding 'ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")',

> The EU Cybersecurity Emergency Fund is an initiative developed in the context of the review of the Cybersecurity Strategy on the example of existing crisis mechanisms in other EU policy areas. It will provide the possibility for Member States to seek help at the EU level in case of major incident. It could be used to support, directly or indirectly, citizens, companies or public administrations hit by cyberattacks, provided that a basic level of cybersecurity protection had been in place before the incident occurred.[669]

More specifically, the fund could 'deploy a rapid response capability in the interests of solidarity and finance specific emergency response actions such as replacing compromised equipment or

[669] Impact Assessment accompanying the document Proposal For a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act") SWD 500/948161 - Part 1, (*European Commission,* 2017) 16.

deploying mitigation or response tools to assist victims.'[670] Use of the fund would be dependent on fulfilling certain security criteria, including 'full implementation of the NIS Directive, mature risk management and respective supervisory frameworks at national level.'[671] As of the writing of this paper, the Commission's proposed Cyber Emergency Fund awaits further development, and further information on the subject is pending.

The Cyber Emergency Fund proposal outlined above implies at least partial public funding.[672] One reason as to why a role for public financing is warranted is that the financial system's cybersecurity vis-à-vis cyber warfare has implications for national and supranational security. As a weapon of states and non-state actors, major cyberattacks warrant a state response where a company's due diligence has already been met and an attack meets the definition of cyber warfare or cyber terrorism. Public funding in this context would mitigate the problems posed by war and terrorism exclusion clauses in private sector insurance.

Nevertheless, this paper agrees with the argument principle that public funding should not be the primary resort.[673] Although high security criteria for access to the fund would mitigate moral hazard—in this case the temptation to invest less in cybersecurity given a financial, EU-level security blanket—private-sector initiatives would mitigate moral hazard more effectively. The exhaustion of relevant private-sector initiatives should, therefore, be a requirement for access to publicly-backed emergency funds.

ii. Singapore's Commercial Cyber Risk Pool

In so far as insurers continue to be reluctant to offer cyber warfare and cyber terrorism insurance by themselves, a commercial cyber risk pool can serve as a private sector mitigant of the relevant exclusion clauses. In 2018, the Monetary Authority of Singapore announced its intention to launch a commercial cyber risk pool to provide cyber insurance to companies regionally.[674]

---

[670] Impact Assessment accompanying the document Proposal For a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act") SWD 500/948161 - Part 1, (*European Commission,* 2017) 48.
[671] ibid.,
[672] ibid., 16; Richard Parlour, Sylvain Bouyon, and Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 35-36.
[673] Richard Parlour, Sylvain Bouyon, and Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 36.
[674] Yakir Golan, '2019 Cyber Insurance Predictions: Strong Drivers For Growth Ahead' (*Insurance Journal*, 15 January 2019) <www.insurancejournal.com/news/international/2019/01/15/514558.htm> accessed 6 March 2020; Gabriel Olano, 'Singapore Launches First Commercial Cyber Risk Pool' (*Insurance Business,* 30 October 2018) <www.insurancebusinessmag.com/asia/news/cyber/singapore-launches-first-commercial-cyber-risk-pool-115040.aspx> accessed 1 August 2020; Heng Swee Keat, 'Speech by Mr Heng Swee Keat, Minister for Finance,

Insurance-linked securities and reinsurance serve as backing for a pool that is expected to reach one billion USD. Twenty insurers were already associated with the pool when the Minister of Finance announced the initiative. Further details for this commercial cyber risk pool are pending.

iii. Suggestions for a European Commercial Cyber Risk Pool

An *EU commercial cyber risk pool composed of private-sector institutions* would offset the European financial system's cyber risk, currently exacerbated by cyber war/terrorism exclusion clauses. The Singaporean initiative could serve as a blueprint for the creation of an EU pool.

- This pool would offer explicit coverage for acts of cyber warfare and cyber terrorism.
- Taking inspiration from the Commission's proposed Cyber Emergency Fund, it would have a rapid response mechanism for covering the infrastructural and operational costs of combatting and recovering from a large-scale cyberattack.
- This rapid response mechanism would buffer a publicly-backed rapid response mechanism (discussed in the next section). While publicly-backed rapid response funding is warranted in cases of cyber warfare and cyber terrorism, a publicly-backed fund's exposure should be limited by first requiring the use of the privately-backed pool.
- (Re)insurers participating in the European commercial pool could consult with relevant EU authorities (e.g., the Commission, EIOPA, ESMA, ENISA, the ECB, the Euro Cyber Resilience Board, the SSM, and a (potential) cyber hub) to develop a range of insurance packages.
- In order to quantify cyber risk and to price premiums, the commercial pool would work closely with the relevant EU and member state agencies to gather and analyse information about cyber infrastructure and risk. Singapore's pool can serve as a model once it is rolled out further and more information is available.
- The commercial pool could additionally offer deposit insurance to participating financial institutions. This insurance would complement the €100,000 cap per deposit that is currently insured by national deposit insurance schemes and will eventually be insured

and MAS' Board Member, at the 15th Singapore International Reinsurance Conference on 29 October 2018' (*Monetary Authority of Singapore,* 29 October 2018) <www.mas.gov.sg/news/speeches/2018/speech-at-the-15th-singapore-international-reinsurance-conference> accessed 5 September 2020.

by the European Deposit Insurance Scheme (discussed further in the next section).[675] This component of the risk pool could be modelled on the Depositors Insurance Fund of the US State of Massachusetts (est. in 1934), which is funded by its private-sector participants.[676]

[675] Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions "Towards the Completion of the Banking Union" [2015] COM/2015/0587 final; Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 806/2014 in order to establish a European Deposit Insurance Scheme [2015] COM/2015/0586.
[676] 'When Protection is Key' (*Depositors Insurance Fund*) <www.difxs.com/DIF/Home.aspx>.

IV.VII. EMERGENCY FUNDS FOR SYSTEMIC CYBER RISK

As discussed in Section III.VII., two significant issues for financial cybersecurity in the context of systemic risk are (1) the ability to rapidly allocate resources to stabilise and defend infrastructure and (2) the ability to resolve and restructure affected banks.[677] Appropriate mechanisms on both counts can help to prevent or mitigate a widespread loss of confidence in the financial system.[678] With respect to the second issue, there are concerns about the adequacy of the Single Resolution Fund (SRF) and the European Stability Mechanism.[679] In the context of bank resolution caused by an act of cyber war/terrorism, one question that arises is whether direct public backing for such a resolution might be warranted, given that the instability is not the result of market behaviour. In light of these issues, this section considers emergency funding frameworks and adjustments to bank resolution financing in the context of cyber-induced systemic instability.

The suggestions put forward in this section include,

- A publicly-backed complement to the commercial cyber risk pool's rapid response mechanism.
- Giving the SRF a degree of public backing in cases where cyber warfare/terrorism induce resolution, given cyber warfare/terrorism's relevance to national security.

i. Rapid Cyber Emergency Funding

As indicated in the preceding section, one method of mitigating cyber-induced systemic risk is to rapidly allocate funds to shore-up affected cyber infrastructure and to '[deploy] mitigation or response tools to assist victims.'[680] Rather than focusing on pre-emption like the Cyber Infrastructure Funds described in Sub-section II.viii., the Commission's proposed Cyber

[677] Commission Working Document Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") [2017] SWD/2017/500 16.
[678] ibid.
[679] Willem Pieter de Groen, 'Financing Bank Resolution: An Alternative Solution for Arranging the Liquidity Required—Banking Union Scrutiny' (*Economic Governance Support Unit: Directorate-General for Internal Policies of the Union*, 2018) 4-9, 11, 16-17.
[680] Impact Assessment accompanying the document Proposal For a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act") - Part 1, [2017] SWD 500/948161 16, 48; Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the policy mix right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 35; Joint Communication to the European Parliament, The European Council and the Council: Resilience, Deterrence, and Defence: Building strong cybersecurity for the EU [2017] JOIN(2017) 7-8.

Emergency Fund outlined in the preceding section would focus on mitigation.[681] It has been suggested that such a fund could operate similarly to the EU Solidarity Fund which provides for natural disasters.[682] A further possibility is that the fund could be financed by both the public and private sectors.[683]

The CEPS-ECRI Task Force emphasises that such a fund should act as reinsurance,[684] meaning that a financial institution's use of the fund would be dependent on first using relevant private insurance mechanisms. The fund would provide relief only after private (re)insurance is spent. Access would also take into account Member States' capacity to quell the situation.[685] The inclination for financial institutions to avoid investing in cybersecurity with the expectation of a publicly funded bail-out would be further reduced by only providing funds to companies that meet set security requirements.[686]

An Emergency Fund Specific to the Financial Sector?

The CEPS-ECRI Task Force has also considered whether the proposed Cyber Emergency Fund should have a variant specific to the financial sector. This additional fund would build up the capacity to combat cyber-induced systemic instability within the financial system and possibly even have a bank resolution function dedicated to bank collapse triggered by cyber incidents.[687]

However, the CEPS-ECRI Task Force has concluded that it is not necessary to establish a fund specific to the financial sector at this time. Although the Task Force recognises the possibility that cyber-attacks could impact the EU financial system in the future, the 'still ambiguous relationship between cyber-risks and systemic risk in the financial sector' informs their conclusion that 'there is no sufficient ground to develop an emergency cyber-fund only for the

[681] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 35.
[682] ibid; Catherine Stupp, 'Ansip: Member States Will Need Help from EU Cyber Emergency Fund' (*Euractiv,* 14 September 2017) <https://www.euractiv.com/section/cybersecurity/news/ansip-member-states-will-need-help-from-eu-cyber-emergency-fund/> accessed 23 September 2020.
[683] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 35.
[684] ibid,36.
[685] Impact Assessment accompanying the document Proposal For a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act") - Part 1 [2017] SWD 500/948161 16, 48.
[686] ibid.
[687] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 38.

financial sector.'[688] Rather, the Task Force suggests that the private sector should have discretion regarding such measures at present.[689]

As an alternative, the Task Force puts its weight behind a fund that covers essential services across various sectors.[690] In covering essential services across various sectors, an overarching Cyber Emergency Fund would be responsive to hybrid attacks. Hybrid threats combine disinformation, attacks on infrastructure, paralysation of public services, traditional military action, and/or cyberattacks.[691] Efforts to combat hybrid attacks are already being pursued at the EU-level. The European Commission is responding to the growing incidence of hybrid threats and established The Hybrid Fusion Cell in 2018.[692] The Hybrid Fusion Cell assesses and seeks to combat such threats.[693] Nevertheless, it is advisable that any cyber fund proposal takes hybrid threats into account, since attacks on other infrastructures exacerbate the cyber elements of such incidents. The CEPS-ECRI proposal for a multi-sectoral cyber fund would complement the Hybrid Fusion Cell's work, which together would facilitate more agile responses to hybrid attacks.

A Cyber Emergency Fund with a Resolution Role?

The Task Force's conclusion about whether to establish a fund specific to the financial sector comes with the implication that a close connection between cyber-attacks and systemic risk could warrant a Cyber Emergency Fund specific to the financial sector that tries to comprehensively combat cyber-induced systemic instability for that sector.[694]

This indication is possibly accompanied by the implication that a close connection between cyber incidents and systemic risk might warrant a Cyber Emergency Fund that couples funding for rapid infrastructural reconstruction with funding for bank resolution caused by cyber-induced

[688] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 36-38.
[689] ibid.
[690] ibid., 38.
[691] Maria Demertzis and Guntram Wolff, 'Hybrid and Cybersecurity Threats and the European Union's financial system', (*Bruegel,* 2019) 3; Damien McGuinness, 'How a Cyber-Attack Transformed Estonia' (*BBC,* 2017) <www.bbc.com/news/39655415> accessed 27 March 2020.
[692] 'A Europe that Protects: EU Works to Build Resilience and Better Counter Hybrid Threats' (*European Commission,* 2018) <https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4123> accessed 27 March 2020; Joint Communication to the European Parliament, The European Council and the Council: 'Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats [2018] JOIN (2018) 16.
[693] Joint Communication to the European Parliament, The European Council and the Council: 'Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats [2018] JOIN (2018) 16; 'A Europe that Protects: EU Works to Build Resilience and Better Counter Hybrid Threats' (*European Commission,* 2018) <https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4123> accessed 27 March 2020.
[694] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 36-38.

insolvency. A resulting inference is that this dual role might also be a possibility in a multi-sectoral cyber emergency fund and could activate when cyber incidents against the financial system occur.

The CEPS-ECRI policy report is, however, ambiguous regarding a Cyber Emergency Fund's intended relationship with a resolution capacity. This is a significant ambiguity about the practicalities of such a fund. In so far as the CEPS-ECRI report does suggest a combined infrastructural/operational response and bank resolution fund, this present paper cautions against such a suggestion. On the one hand, such a fund would have freedom to financially handle cyber incidents in the financial sector holistically in so far as its resources allow. Given concerns about the adequacy of the existing SRF, however (see Sub-section III.VII.v.),[695] a Cyber Emergency Fund that seeks to cover cyber-induced resolution has a high risk of running out of resources. Since a resolution fund already exists, there is little reason to establish a specific cyber fund that combines other emergency functions with a resolution role. Resolution funds dedicated to specific underlying causes concentrate the risk pool unnecessarily. Therefore, this paper suggests a Cyber Emergency Fund that does not offer deposit insurance or resolution mechanisms.

An Agile, Publicly-Backed Cyber Emergency Fund in Cooperation with the Commercial Pool

Systemic risk warrants a rapid response fund for mitigating the infrastructural and operational ramifications of cyber warfare/terrorism.[696] A publicly-backed Cyber Emergency Fund for such purposes would offer an additional layer of resources for rapid response beyond those of a commercial pool. A role for public financing is warranted in so far as an act of cyber war/terrorism that causes systemic instability is a national and EU-wide security risk with geopolitical implications.

- *A multi-sectoral Cyber Emergency Fund* that covers a range of essential services would further diversify the risk portfolio and would be more responsive to hybrid attacks than a fund specific to the financial sector.[697] Whereas the CEPS-ECRI Task Force sees a connection between cyber and systemic risk as cause for creating a fund specific to the

[695] Willem Pieter de Groen, 'Financing bank resolution: An Alternative Solution for Arranging the Liquidity Required—Banking Union Scrutiny' (*Economic Governance Support Unit: Directorate-General for Internal Policies of the Union*, 2018) 4-9.
[696] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 35-37.
[697] Ali Ahangar et al., 'Why Are Risk-Pooling and Risk-Sharing Arrangements Necessary for Financing Healthcare and Improving Health Outcomes in Low and Lower Middle-Income Countries' [2018] *Health* 10 124-125.

financial sector (see Sub-section IV.VII.i.), this paper recommends a broader fund in light of that connection.

The success of the Solidarity Fund indicates the EU's effective deployment of centralised emergency funds. This experience lessens potential concerns about the operational difficulties of unitary funds for which there is a noteworthy literature with respect to healthcare.[698]

- The publicly-backed Cyber Emergency Fund would be *separate to the Solidarity Fund* because the latter is an ex-post fund rather than one for agile response.

- Access to the public Cyber Emergency Fund would depend on first exhausting the *commercial risk pool's rapid response mechanism* (see Sub-section IV.VI.iii.) and those of *any other privately-backed rapid response initiatives*.

  This stands in contrast to a single (privately and publicly) co-financed fund in which all contributions are pooled for direct use (as suggested by the CEPS-ECRI report).[699] Rather, separate public and private arms of European rapid response funding would work in partnership with one another.

  They would also work co-operatively with operators of essential services as well as with the existing CSIRTs Network (or with a potential cyber hub).

  In addition to baseline security and due diligence criteria for access to a Cyber Emergency Fund, the requirement for first recourse to private rapid response funding would incentivise companies to invest in their cybersecurity. This requirement would reduce moral hazard. The requirement would also spur the growth of a cyber insurance market that takes cyber warfare and cyber terrorism into account.

- Such a fund would take into account victims' *prior due diligence* and *national response capacities,* as suggested by the European Commission's Impact Assessment. [700]

[698] Ali Ahangar et al., 'Why Are Risk-Pooling and Risk-Sharing Arrangements Necessary for Financing Healthcare and Improving Health Outcomes in Low and Lower Middle-Income Countries' [2018] *Health* 10 124-125; Commission Staff Working Document Executive Summary of the Evaluation of the European Union Solidarity Fund 2002-2017 SWD/2019/186 final 3-4.
[699] Richard Parlour, Sylvain Bouyon, Simon Krause, *Cybersecurity in Finance, Getting the Policy mix Right!–Report of a CEPS-ECRI Task Force* (CEPS-ECRI, 2018) 38.
[700] Impact Assessment accompanying the document Proposal For a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on

- The Cyber Emergency Fund's 'rapid response capability'[701] could include the *agile assessment and provision of necessary funds in response to each incident reporting stage*. This process would be facilitated by the cyber hub framework developed in Section IV.I. Both the private and public sides of the suggested rapid emergency response framework could work closely with a potential cyber hub.

- Both the privately and publicly-backed rapid response funds could have *ex post reinsurance from the private sector.*

ii. Co-Financed Resolution due to Cyber Warfare/Terrorism

In the event that rapid response measures, private sector (re)insurance, and initial European Deposit Insurance are not able to prevent a bank's resolution, an additional element of public funding could complement the Single Resolution Fund and ESM in cases of cyber warfare or cyber terrorism. This could involve an additional layer of direct public backing within the ESM for use in cases of resolution caused by cyber warfare or cyber terrorism.

- Such an element of public backing is warranted for cyber-attacks that amount to warfare or terrorism. Cyber terrorism and warfare against the financial sector can become a national and supranational security issue. As weapons of state and non-state actors, such incidents warrant a state response when a financial institution's due diligence has already been met and non-publicly funded (re)insurance and resolution mechanisms have been exhausted.

- Access to public funds for bank resolution in cases of cyber warfare/terrorism would be predicated on regulation that requires all financial institutions with subsidiaries or headquarters in an EU member state to participate in the European commercial cyber risk pool suggested in the preceding section. Alternatively, they would need to demonstrate appropriate private sector insurance for cyber warfare and terrorism.

Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act") - Part 1 [2017] SWD 500/948161 48.

[701] Joint Communication to the European Parliament, The European Council and the Council: Resilience, Deterrence, and Defence: Building Strong Cybersecurity for the EU [2017] JOIN (2017) 7-8.

V. CONCLUDING REMARKS

Of the many issues affecting financial cybersecurity in the Eurozone, this paper has focused on the issue of harmonisation/fragmentation, cyber-induced (systemic) risk, and the relationship between regulation and emerging technology; policy themes that the 2008-2012 Global Financial Crisis, the growth of cross-border cyber incidents, and the rapidly developing financial technology landscape have brought to the fore. These are overlapping issues that are important for financial stability in the Eurozone.

Fragmented information sharing and incident and vulnerability reporting frameworks contribute to inefficient assessment and handling of cross-border incidents. The relationship between regulation and emerging financial technologies (e.g., decentralised ones) also has an important impact on the financial cybersecurity landscape. Software and operational vulnerabilities in emerging fintech, and in their interfaces with legacy/existing technologies, can be further exacerbated by legislative gaps/grey-zones and by unharmonized cross-national policies. Effective mitigants on the financial side are also imperative for financial cybersecurity, and insurance clauses that exclude acts of cyber warfare and cyber terrorism have the potential to leave financial institutions further exposed. These policy areas become even more pressing in light of the growing recognition of, and attention to, cyber-induced systemic risk. Strengthening all these areas can help to mitigate and/or prevent the proliferation of cyber-induced financial instability.

The EU and the Eurozone are complex projects. This paper recognises that a delicate balance needs to be struck between harmonisation and autonomy. An attempt has been made to take systemic, member state, sectoral, and sub-sectoral interests into account. While the policy suggestions put forward in this paper tend towards greater harmonisation, this paper pursues that harmonisation by offering both more and less centralising suggestions that can complement one another.

Many of the suggestions in this paper reinforce one another and can be pursued in parallel. The financial system can be reinforced against cyber-induced systemic risk by further harmonising incident and vulnerability reporting, improving information sharing, developing appropriate cyber insurance and rapid response funds, and adjusting existing resolution mechanisms. More harmonised incident and vulnerability reporting facilitates stronger third-party+ oversight and vice versa. A more cohesive reporting and information sharing framework is also of use to a cyber insurance market that suffers from information asymmetry.

In a financial system that is continually shaped by emerging financial technologies, improving cooperation between regulators and fintech developers can result in frameworks that facilitate more thorough and efficient incident and vulnerability reporting. Such efforts can also benefit the cyber insurance market, which needs to have reference to criteria by which it can price insurance. Softly-centralised governance for unconventional fintech that are being integrated into the mainstream financial system has the potential to improve incident and vulnerability reporting for the emerging components and for their interfaces with legacy systems. Improving reporting in these areas further reduces the potential for incidents that might lead to systemic instability.

In the rapidly developing technological landscape, the number of important policy areas for reinforcing cybersecurity in the Eurozone abound. This paper has covered a selection of these issues with the aim of providing a point of reference for cybersecurity reinforcement in these areas. Financial cybersecurity is an issue that touches the lives of everyone engaged in the modern financial system. The suggestions contained in this paper aim to help avoid and manage a potential cyber-induced financial crisis and to reduce more localised financial risks that can have momentous repercussions on the lives of affected individuals.

VI. BIBLIOGRAPHY

Primary Sources:

Consolidated Version of the Treaty on European Union [2012] OJ C.

Commission Decision of 5.7.2016 on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation C/2016/4400 final.

Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact [2018] OJ L 26 [2004] OJ L 77.

Commission Recommendation of 9 April 2014 on the quality of corporate governance reporting ('comply or explain') Text with EEA relevance [2014] OJ L 109.

Commission Staff Working Document Executive Summary of the Evaluation of the European Union Solidarity Fund 2002-2017 SWD/2019/186 final.

Commission Staff Working Document Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres [2018] SWD/2018/403 final.

Commission Staff Working Document Impact Assessment accompanying the document Proposal For a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") SWD/2017/500.

Communication from the Commission on the EU Security Union Strategy [2020] COM(2020) 605 final.

Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions "Towards the Completion of the Banking Union" [2015] COM/2015/0587 final.

Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions FinTech Action plan: For a more competitive and innovative European financial sector [2018] COM/2018/0109.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions [2015] COM/2015/0185 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions the European Agenda on Security COM/2015/0185 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Single Market Strategy for Europe [2015] SWD/2015/100 final.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) [2016] OJ L 194.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201.

Directive 2006/46/EC of the European Parliament and of the Council of 14 June 2006 amending Council Directives 78/660/EEC on the annual accounts of certain types of companies, 83/349/EEC on consolidated accounts, 86/635/EEC on the annual accounts and consolidated accounts of banks and other financial institutions and 91/674/EEC on the annual accounts and consolidated accounts of insurance undertakings (Text with EEA relevance) [2006] OJ L 224.

Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities [2017] DGD 2B/13007/17.

Draghi, Mario, 'Speech by Mario Draghi, President of the European Central Bank at the Global Investment Conference in London 26 July 2012' (*European Central Bank*, 26 July 2012) <www.ecb.europa.eu/press/key/date/2012/html/sp120726.en.html> accessed 19 September 2020.

EU Cyber Defence Policy Framework (2018 update) [2018] RELEX.2.B/14413/18.

EU Cyber Defence Policy Framework [2014] DG C 2B 15585/14 Annex.

Explanatory Memorandum to the Civil Aviation (Contributions to the Air Travel Trust Regulations) [2007] No. 2999.

General Secretariat of the Council, 'Council Conclusions on Regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age' [2020] 13026/20.

Heng, Swee Keat, 'Speech by Mr Heng Swee Keat, Minister for Finance, and MAS' Board Member, at the 15th Singapore International Reinsurance Conference on 29 October 2018' (*Monetary Authority of Singapore,* 29 October 2018) <https://www.mas.gov.sg/news/speeches/2018/speech-at-the-15th-singapore-international-reinsurance-conference> accessed 5 September 2020.

ISO/IEC 27035:2011 Annex D.4.

Impact Assessment accompanying the document Proposal For a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('"Cybersecurity Act"') - Part 1, [2017] SWD 500/948161

Joint Communication to the European Parliament and the Council: Joint Framework on Countering Hybrid Threats a European Union response [2016] JOIN(2016) 18 final.

Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade [2020] JOIN 18 final.

Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN/2013/01 final.

Joint Communication to the European Parliament, The European Council and the Council: Resilience, Deterrence, and Defence: Building Strong Cybersecurity for the EU [2017] JOIN(2017).

Joint Communication to the European Parliament, The European Council and the Council: Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats [2018] JOIN(2018).

Joint Staff Working Document Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats [2019] SWD(2019) 200 final.

Lagarde, Christine, 'Remarks on the Occasion of Receiving the Grand Prix de l'Économie 2019 from Les Echos', (*European Central Bank*, 2020) <www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200205_1~cc8a8787f6.en.html> accessed 28 February 2020.

Ministerie van Defensie Kamerbrief en Convenant Joint Sigint Cyber Unit (JSCU) [2014].

Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 806/2014 in order to establish a European Deposit Insurance Scheme [2015] COM/2015/0586.

Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018 [2018] COM/2018/630.

Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology COM(2020) 594 final.

Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, 2020/0266 (COD).

Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 COM(2020) 593 final.

Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 COM(2020) 823 final.

Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency [2004] OJ L 77.

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] OJ L 119/1.

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] OJ L 151.

The Financial Services Innovation Act of 2016 H.R. (114th Cong. 2016) 6118.

Treaty No. 185 The Convention on Cybercrime of the Council of Europe [2001] ETS 185.

'United Nations Convention Against Transnational Organized Crime and the Protocols Thereto' (*United Nations: Office on Drugs and Crime*, 2004).

Secondary Sources:

'33 New EU Funded Projects to Assist EU Member States in Building up their Cybersecurity Capabilities' (*European Commission,* 30 April 2019) <https://ec.europa.eu/digital-single-market/en/news/33-new-eu-funded-projects-assist-eu-member-states-building-their-cybersecurity-capabilities> accessed 01 March 2020.

'A Europe that Protects: EU Works to Build Resilience and Better Counter Hybrid Threats' (*European Commission,* 2018) <https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4123> accessed 27 March 2020.

'About' (*B-Hub: Blockchain for Europe*) <https://b-hub.eu/about/> accessed 27 December 2020.

'About' (*EBOF*) <www.eublockchainforum.eu/about> accessed 06 October 2020.

'About ECSO' (*European Cyber Security Organisation*) <https://ecs-org.eu/about> accessed 22 September 2020.

'About ENISA – The European Union Agency for Cybersecurity: Towards a Trusted and Cyber Secure Europe' (*ENISA,* 2020) <https://www.enisa.europa.eu/about-enisa> accessed 02 August 2020.

'About Us' (*European Stability Mechanism*) <https://www.esm.europa.eu/about-us/intro> accessed 01 August 2020.

'A Crypto-Decentralist Manifesto' (*Ethereum Classic*, 11 July 2016) <https://ethereumclassic.org/blog/2016-07-11-crypto-decentralist-manifesto> accessed 08 October 2020.

Ahangar, A et al., 'Why Are Risk-Pooling and Risk-Sharing Arrangements Necessary for Financing Healthcare and Improving Health Outcomes in Low and Lower Middle-Income Countries' [2018] *Health* 10.

Ahmed, M S, and B Dyson, 'Cyber insurance wrestle with war exclusions as state-sponsored attack fears grow' (*S&P Global Market Intelligence*, 30 January 2020) <www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyber-insurers-wrestle-with-war-exclusions-as-state-sponsored-attack-fears-grow-56743302> accessed 25 September 2020.

Ali, R, 'Cellular structure for a Digital Fiat Currency' (*P2P Financial System International Workshop, Federal Reserve Bank of Cleveland*, 2018).

Allen, F, et al., *Cross-Border Banking in Europe: Implications for Financial Stability and Macroeconomic Policies* (Centre for Economic Policy Research, 2011).

Article 19 Incident Reporting: Incident Reporting Framework for eIDAS Article 19 (ENISA, 2016).

Ashton, M, *What's Wrong With Money?: The Biggest Bubble Of All* (John Wiley & Sons, 2016).

Basak, S, 'Worried About a Cyber-Apocalypse? AIG Wants to Sell You a Policy' (*Bloomberg*, 22 July 2015), <www.bloomberg.com/news/articles/2015-07-22/worried- about-a-cyber-apocalypse-aig-wants-to-sell-you-a-policy> accessed 19 September 2020.

Bacon, J, et al., 'Blockchain Demystified: A Technical and Legal Introduction to Distributed And Centralised Ledgers' (2018) 25 Rich JL & Tech.

Barlow, H, 'The Race to Regulate: Can the Law Keep Pace with Technology Innovation?' (*JDX Consulting,* 8 August 2019) <www.jdxconsulting.com/technology/the-race-to-regulate-can-the-law-keep-pace-with-technology-innovation/> accessed 20 October 2020.

'Become a Member' (*FS-ISAC*) <www.fsisac.com/membership> accessed 1 November 2020.

Biryukov, A, et al., 'Deanonymisation of clients in Bitcoin P2P network' (*Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014).

'Bitcoin Improvement Proposals' (*Github*) <https://github.com/bitcoin/bips > accessed 08 October 2020.

'Bitcoincash' (*BitcoinCash*) <www.bitcoincash.org/faq/> accessed 08 October 2020.

'Blockchain HUB FOR EUROPEan Startups Acceleration and Growth' (*European Commission: CORDIS EU research results*, 03 July 2020) <https://cordis.europa.eu/project/id/871869> accessed 27 December 2020.

'Blockchain Technologies' (*European Commission*, 2020) <https://ec.europa.eu/digital-single-market/en/blockchain-technologies> accessed 07 March 2020.

Blyth, M, *Austerity: The History of a Dangerous Idea* (Oxford University Press, 2013).

Bouca, Ca, 'EU GDPR Controller Vs. Processor – The Differences' (*Advisera Expert Solutions Ltd.,* 2020) <https://advisera.com/eugdpracademy/knowledgebase/eu-gdpr-controller-vs-processor-what-are-the-differences/> accessed 27 February 2020.

Bracher, P, 'Cyber Insurance and the War Exclusion | Financial Institutions Legal Snapshot' (*Norton Rose Fulbright: Financial Institutions Legal Snapshot*, 16 July 2019) <www.financialinstitutionslegalsnapshot.com/2019/07/cyber-insurance-and-the-war-exclusion/> accessed 06 March 2020.

Broughton, K, 'Crypto Firms Assess How to Comply With Anti-Money-Laundering Standards' (*The Wall Street Journal*, 16 September 2019) <www.wsj.com/articles/crypto-firms-assess-how-to-comply-with-anti-money-laundering-standards-11568626200> accessed 16 December 2020.

Butler, D, 'A World Where Everyone Has a Robot: Why 2040 Could Blow Your Mind' (*Nature*, 24 February 2016) <www.nature.com/news/a-world-where-everyone-has-a-robot-why-2040-could-blow-your-mind-1.19431> accessed 21 October 2020.

'Can SWIFT help with Blockchain Interoperability?' (Ledger Insights) <www.ledgerinsights.com/can-swift-help-with-blockchain-interoperability/> accessed 01 October 2020.

Carrapico, H, and Andre B, 'The EU as a Coherent (Cyber)Security Actor' [2017], JCMS *55*(6).

Chang, Y, et al.,' Blockchain in Global Supply Chains and Cross Border Trade: A Critical Synthesis of the State-of-the-Art, Challenges and Opportunities' [2020] *58*(7) International Journal of Production Research.

CERT Capability Team, 'Good Practice Guide on Vulnerability Disclosure: From challenges to recommendations' (*ENISA*, 2015).

'Challenges to Effective EU cybersecurity policy' (*European Court of Auditors* 2019).

Christie, R, *Safeguarding the Euro in Times of Crisis: The inside story of the ESM* (European Stability Mechanism, 2019).

Ciobanu, C, 'Good Practice Guide on Vulnerability Disclosure' (*ENISA,* 2015).

CIO Experience Group Information Security, 'Coordinated Vulnerability Disclosure: Model Policy and Procedure' (*CIO Platform Nederland: CEG Information Security*, 2016).

'CISA Coordinated Vulnerability Disclosure (CVD) Process' (*Cybersecurity and Infrastructure Security Agency, Department of Homeland Security,* 3 December 2019)

<https://www.cisa.gov/coordinated-vulnerability-disclosure-process> accessed 28 April 2020.

Clarke, R A., and R Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (Harper Collins, 2010).

Clozel, L, 'OCC's Curry Rules Out 'Safe Space' for FinTech Companies' (*American Banker*, 03 November 2016).

Cohn, C, 'Terrorism Reinsurance Fund in UK Wants to Add Cyber Cover' (*Carrier Management*, 10 March 2017) <www.carriermanagement.com/news/2017/03/10/165134.htm> accessed 19 September 2020.

Collingridge, D, *The Social Control of Technology* (Open University Press, 1981).

'Commission Welcomes Political Agreement on the Cybersecurity Competence Centre and Network' (*European Commission*, 11 December 2020) <https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2384> accessed 20 December 2020.

'Complete Guide to GDPR compliance', (*GDPR*, 2020) < https://gdpr.eu/ > accessed 08 October 2020.

Computer Crime & Intellectual Property Section (Criminal Division), 'A Framework for a Vulnerability Disclosure Program for Online Systems' (*U.S. Department of Justice,* 2017).

'Connecting Europe Facility' (*European Commission*) <https://ec.europa.eu/inea/en/connecting-europe-facility> accessed 20 December 2020.Coppola, Frances, 'SWIFT's Battle for International Payments'. (*Forbes*, 16 July 2019) <https://www.forbes.com/sites/francescoppola/2019/07/16/swifts-battle-for-international-payments/#1162a9dc758e> accessed 30 September 2020.

'Coordinated Vulnerability Disclosure Manifesto Signed', (*Radobank,* 2016) <https://www.rabobank.com/en/press/search/2016/20160512-coordinated-vulnerability-disclosure-manifesto.html> accessed 01 May 2020.

'Coordinated Vulnerability Disclosure: Guidelines published by the NCSC', (*ENISA,* 2018) <https://www.enisa.europa.eu/news/member-states/coordinated-vulnerability-disclosure-guidelines-published-by-ncsc> accessed 03 May 2020.

'Coordinated Vulnerability Disclosure' (*Microsoft Security Response Center*) <https://www.microsoft.com/en-us/msrc/cvd> accessed 24 April 2020.

'Corporate Governance: European Forum Clarifies 'Comply or Explain' principle and issues annual report' (*European Commission,* 6 March 2006) <https://ec.europa.eu/commission/presscorner/detail/en/IP_06_269> accessed 18 September 2020.

'Cost of a 51% Attack for Different Cryptocurrencies | Crypto51' (*Crypto51.app*, 2020) <https://www.crypto51.app/> accessed 27 February 2020.

Courcelas, L, T Lyons, and K Timsit, 'The EU Blockchain Observatory and Forum, Conclusions and Reflections 2018-2020 (*EBOF*, 2020).

Cowhey, P F., J D. Aronson, *Digital DNA: Disruption and the Challenges for Global Governance* (Oxford University Press, 2017) ch 7.

Cox, T and A Solomon, 'Blockchain: Is the GDPR Already Outdated?' (*Tech Law for Everyone*, 5 September 2017) <www.scl.org/articles/9994-blockchain-is-the-gdpr-already-outdated> accessed 08 October 2020.

'Cryptocurrency Anti-Money Laundering Report 2018' (*Ciphertrace.com*, 2018) <https://ciphertrace.com/crypto-aml-report-2018q3.> accessed 27 February 2020.

'Cryptojacking - Cryptomining In the Browser' (*ENISA,* 10 November 2017) <https://www.enisa.europa.eu/publications/info-notes/cryptojacking-cryptomining-in-the-browser?fbclid=IwAR0h32Ir23DAyp0RLYO_hiGgTiNpmkQ21V1gjK3IESKsTreQKvy9xRIbndE> accessed 27 February 2020.

'CSIRTs Network' (*CSIRTs Network*) <https://csirtsnetwork.eu/> accessed 20 July 2020.

'Cyber and Privacy Insurance' (*IRMI*) <https://www.irmi.com/term/insurance-definitions/cyber-and-privacy-insurance> accessed 01 March 2020.

'Cyber Resilience and Financial Market Infrastructures', (*European Central Bank*, 2020) <www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html> accessed 10 March 2020.

'Cyber risks – Insurable, But Within Limits' (*Swiss Re*) <www.swissre.com/reinsurance/property-and-casualty/solutions/cyber-solutions/cyber-risks-insurable-but-within-limits.html> accessed 23 September 2020.

'Cybersecurity Institutional Map' (*ENISA*) <www.enisa.europa.eu/about-enisa/cybersecurity-institutional-map/results> accessed 20 December.

'Cyber Threat Real-Time Map' (Kaspersky, updated continuously) <https://cybermap.kaspersky.com/> accessed 23 September 2020.

'Cyber Warfare' (*RAND Corporation*, 2020) <www.rand.org/topics/cyber-warfare.html> accessed 14 April 2020.

'Cybercrime', (*European Commission*) <https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en> accessed 10 March 2020.

'Cybersecurity Education' (*ENISA,* 2020) <https://www.enisa.europa.eu/topics/cybersecurity-education> accessed 01 August 2020.

Cybersecurity Technology and Capacity Building Unit, 'The Cybersecurity Act' (*European Commission* 28 February 2020) <https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act> accessed 10 September 2020.

Cybersecurity Technology and Capacity Building Unity, 'Proposal for a European Cybersecurity Competence Network and Centre' (*European Commission,* 19 September 2018) <https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre> accessed 01 August 2020.

De Grauwe, P, *Economics of Monetary Union* (Oxford University Press, 2018).

De Groen, W.P, 'Financing Bank Resolution: An Alternative Solution for Arranging the Liquidity Required—Banking Union Scrutiny' (*Economic Governance Support Unit: Directorate-General for Internal Policies of the Union*, 2018).

De Nederlandsche Bank and AFM, 'More Room for Innovation in the Financial Sector: Market Access, Authorisations and Supervision—Next Steps (*AFM—DNB* ,2016).

'Decentralised Financial Technologies: Report on Financial Stability, Regulatory and Governance Implications' (*Financial Stability Board,* 2019).

De Groot, J, 'What is a Security Operations Center (SOC)?' (*Digital Guardian*, 25 November 2020) <https://digitalguardian.com/blog/what-security-operations-center-soc> accessed 20 December 2020.

Demertzis, M and Guntram W, 'Hybrid and cybersecurity threats and the European Union's financial system' (*Bruegel*, 2019).

Dickson, B, 'Software Vulnerability Disclosure is a Real Mess' (*PCMag UK,* 17 August 2019) <https://uk.pcmag.com/news-analysis/122173/software-vulnerability-disclosure-is-a-real-mess> accessed 01 May 2020.

'Digital Europe Programme: A Proposed €7.5 billion of funding for 2021-2027' (*European Commission*, 4 June 2020) <https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu82-billion-funding-2021-2027> accessed 20 December 2020.

'Distributed Ledger Technology & Cybersecurity: Improving Information Security in the Financial Sector' (*ENISA*, 2016).

Donnelly, G, 'A Manifesto for the Next 10 Years of Bitcoin' (*Cash*, September 2020) <https://read.cash/@georgedonnelly/a-manifesto-for-the-next-10-years-of-bitcoin-cash-c67d115a > accessed 08 October 2020.

'EBF Position Paper on Cyber Incident Reporting' (*European Banking Federation*, 2019).

'ECB Announces Support for FintechBank Applicants' (*Lantham & Watkins LLP*, 20 November 2017), <www.latham.london/2017/11/ecb-announces-support-for-fintech-bank-applicants> accessed 01 June 2020.

'ECSO Position Paper on Sector-Specific ISACs' (*ECSO,* 2018).

Engineer, M.H., P Schure, and M Gillis, 'A Positive Analysis of Deposit Insurance Provision: Regulatory Competition among European Union Countries' [2013] JFS 9(4).

'ENISA Launches Public Consultation for First Candidate Cybersecurity Certification Scheme' (*ENISA*, 2 July 2020) <https://www.enisa.europa.eu/news/enisa-news/enisa-launches-public-consultation-for-first-candidate-cybersecurity-certification-scheme> accessed 10 September 2020.

'EU Budget for the Future' (*European Commission*, 2020)

'EU Global Strategy' (European Union External Action) <https://eeas.europa.eu/topics/eu-global-strategy_en?page=1> accessed 21 September 2020.

'EU National Strategies' (*CyberWISER.eu: Cyber Range and Capacity Building in Cybersecurity*, 2018) <www.cyberwiser.eu/cartography> accessed 20 April 2020.

European Banking Federation, 'EBF Position Paper on Cyber Incident Reporting' (2019) 1-6; Vangelis Ouzounis, 'Good Practice Guide on Reporting Security Incidents', (*ENISA,* 2009).

European Banking Federation, *EBF Position Paper on Cyber Incident Reporting* (2019).

'European Deposit Insurance Scheme: A Proposed Scheme to Protect Retail Deposits in the Banking Union' (*European Commission*) <https://ec.europa.eu/info/business-economy-euro/banking-and-finance/banking-union/european-deposit-insurance-scheme_en#overview> accessed 21 September 2020.

European Insurance and Occupational Pensions Authority, *Cyber Risk for Insurers—Challenges and Opportunities* (2019)

European Insurance and Occupational Pensions Authority, *Understanding Cyber Insurance—A Structure Dialogue with Insurance Companies* (2018).

European Securities and Markets Authorities, European Banking Authority, European Insurance and Occupational Pensions Authority, 'Report—FinTech: Regulatory sandboxes and innovation hubs' [2018] JC 74.

European Stability Mechanism, 'How we work' <www.esm.europa.eu/about-us/how-we-work#overview> accessed 8 December 2020.

European Systemic Risk Board, *Systemic Cyber Risk* (2020).

'European Union Agency for Cybersecurity (ENISA)', (*Official Website of the European Union,* 6 January 2020) <https://europa.eu/european-union/about-eu/agencies/enisa_en> accessed 24 January 2020.

'Experts Letter on the Importance of Security Research' (*Center For Democracy* & Technology, 10 April 2018) <https://cdt.org/insights/experts-letter-on-the-importance-of-security-research/> accessed 01 November 2020.

FATF, '12-Month Review of The Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers' (FATF, 2020) <www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html> accessed 06 November 2020.

Fenwick, M D., W A. Kaal, E P. M. Vermeulen, 'Regulation Tomorrow: What Happens When Technology Is Faster than the Law?' [2017] *American University Business Law Review* 6,3.

Finck, M, 'Blockchain and the General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law? (European Parliament, 2019)

Finley, K, 'A $50 Million Hack Just Showed That the DAO Was All Too Human' (*Wired,* 18 June 2016) <https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/> accessed 10 March 2020.

'FireEye Cyber Threat Map' (*FireEye*, updated continuously) <www.fireeye.com/cyber-map/threat-map.html> accessed 23 September 2020.

Francois, A, 'Is Blockchain the Perfect Defense Against DDos Attacks?' (*PenTest Magazine*, 25 September 2019) <https://pentestmag.com/is-blockchain-the-perfect-defense-against-ddos-attacks/> accessed 27 February 2020.

Frankenfield, J, '51% Attack', (*Investopedia,* 2019) <https://www.investopedia.com/terms/1/51-attack.asp> accessed 29 February 2020.

'From the Netherlands Presidency of the EU Council: Coordinated vulnerability disclosure Manifesto signed', (*ENISA,* 2016) <https://www.enisa.europa.eu/news/member-

states/from-the-netherlands-presidency-of-the-eu-council-coordinated-vulnerability-disclosure-manifesto-signed> accessed 1 May 2020.

Frunza, M-C, *Solving Modern Crime In Financial Markets* (Academic Press 2015).

Gabel, D and M Schuba, 'Germany Rolls out IT Security Act' (*White & Case,* 18 August 2015) <https://www.whitecase.com/publications/article/germany-rolls-out-it-security-act> accessed 13 May 2020

'Gartner Predicts 90% of Blockchain-Based Supply Chain Initiatives Will Suffer 'Blockchain Fatigue' by 2023' (Gartner, 7 May 2019) <www.gartner.com/en/newsroom/press-releases/2019-05-07-gartner-predicts-90--of-blockchain-based-supply-chain> accessed 06 October 2020.

'GDPR Tracker' (*Bird & Bird*) <https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker> accessed 10 September 2020.

'General Data Protection Regulation: GDPR' (*GDPR Info*) < https://gdpr-info.eu/ > accessed 08 October 2020.

'Germany' (*Bird & Bird*) <https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/germany> accessed 10 September 2020.

Gevers, R, et al., 'Coordinated Vulnerability Disclosure: The Guideline' (*National Cyber Security Centre NL, Ministry of Justice and Security,* 2019).

Golan, Y, '2019 Cyber Insurance Predictions: Strong Drivers for Growth Ahead' (*Insurance Journal*, 15 January 2019) <www.insurancejournal.com/news/international/2019/01/15/514558.htm> accessed 06 March 2020.

Górniak, S, 'ENISA in the EU Cybersecurity Certification Framework' Presentation at the IHE Europe Symposium (Rennes, 09 April 2019).

'Governance Working Group' (*INATBA*) <https://inatba.org/working-groups/governance-working-group/> accessed 20 December 2020.

Gray, A, 'Cyber Risks Too Big to Cover, says Lloyd's Insurer: Governments Should Step in to Provide Aid, Says Catlin Boss' (*Financial Times*, 5 February 2015) <https://www.ft.com/content/94243f5a-ad38-11e4-bfcf-00144feab7de> accessed 20 September 2020.

Greenberg, A, 'The Shadow Broker Mess Is What Happens When the NSA Hoards Zero-Days' (*Wired,* 17 August 2016) <www.wired.com/2016/08/shadow-brokers-mess-happens-nsa-hoards-zero-days/> accessed 01 July 2020.

——, 'Hold North Korea Accountable for Wannacry—And The NSA, Too' (*Wired*, 19 December 2017) <https://www.wired.com/story/korea-accountable-wannacry-nsa-eternal-blue/?fbclid=IwAR2Uq1_VRe7XjhTCrmIcq6KYWN88ChNrn4UzoxfpOLDNfmWUB_EU_LEjngs> accessed 27 February 2020

—— , 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History' (*Wired,* 22 August 2018) <www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> accessed 21 May 2020.

Gros, D, and D Schoenmaker, 'European Deposit Insurance and Resolution in the Banking Union' [2014] *JCMS*, 52,3.

'Guidelines for SMEs on the Security of Personal Data Processing' (*ENISA,* 2016) <www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing> accessed 29 January 2020.

Hanselmann, S, 'What is the FATF Travel Rule?' (*Bitcoin Suisse*) <www.bitcoinsuisse.com/research/specials/what-is-the-fatf-travel-rule> accessed 16 December 2020.

Hammerschmidt, C, 'Consensus in Blockchain Systems. In Short.' (*Medium,* 27 January 2017) <https://medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe> accessed 06 October 2020.

Herpig, S, and A Schwartz, 'The Future of Vulnerabilities Equities Processes Around the World (*Lawfare Institute*, 4 January 2019) <www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world> accessed 13 March 2020.

Heywood, D, 'Cybersecurity, data breach, and incident reporting under the GDPR and NISD' (*Taylor Wessing,* March 2018) <www.taylorwessing.com/download/article-cybersecurity-data-breach-and-incident-reporting.html> accessed 21 October 2020.

HM Government Department for Digital, Culture, Media, and Sport, 'Cyber Security Regulation and Incentives Review' (2016) 3.

Hoeppner, S, and Christian K, 'Ex ante versus Ex post Governance: A Behavioral Perspective' [2016], *Review of Law and Economics,* 12,2.

'Home' (*Information Commissioner's Office*) <https://ico.org.uk/> accessed 10 September 2020.

Householder, A. D., G Wassermann, A Manion, and C King, 'The CERT® Guide to Coordinated Vulnerability Disclosure' (*Software Engineering Institute*, 2017).

'How the Blockchain Will Impact the Financial Sector' (*Knowledge@Wharton* 16 November 2018) <https://knowledge.wharton.upenn.edu/article/blockchain-will-impact-financial-sector/> accessed 10 September 2020.

Hurst, A, 'Determining and Overcoming Blockchain Fatigue' (*Information Age*, 21 July 2020) < www.information-age.com/determining-overcoming-blockchain-fatigue-123490369/> accessed 06 October 2020.

'INATBA MiCA Task Force' (*INATBA*) <https://inatba.org/mica-task-force/> accessed 27 December.

'Incident Reporting Template' (*Monetary Authority of Singapore,* 21 June 2013) <https://www.mas.gov.sg/regulation/forms-and-templates/incident-reporting-template> accessed 10 March 2020.

'Information Sharing and Analysis Centres: Cooperative Models' (*ENISA,* 2018).

'Insider and Third-Party Access Rank as Top Cyber Threats for Global Organizations' (*BeyondTrust*, 9 May 2017) <https://www.beyondtrust.com/press/secure-access-report> accessed July 20, 2020.

'Is Blockchain Fatigue Really Going to Set in by 2022?' (*Asia Blockchain Review*, 18 February 2020) <www.asiablockchainreview.com/is-blockchain-fatigue-really-going-to-set-in-by-2022/> accessed 06 October 2020.

Ishii, Y, 'Blockchain Technology and Anti-Money Laundering Regulations under International Law' (*American Society of International Law*, 22 February 2019) <www.asil.org/insights/volume/23/issue/1/blockchain-technology-and-anti-money-laundering-regulations-under#_edn2> accessed 08 October 2020.

Johnston, F, 'Cyberwar/Cyberterrorism—A Challenge for Insurers and Cross-Border Investors' (*RobertWray PLLC*, 28 May 2019) <www.robertwraypllc.com/cyberwar-cyberterrorism-a-challenge-for-insurers-and-cross-border-investors/> accessed 25 September 2020.

Kashyap, M, et al., 'Blurred lines: How FinTech is Shaping Financial Services—Global FinTech Report', (*PWC*, 2016).

Kelly, J, 'Blockchain: disillusionment descends on financial services' (*Financial Times*, 24 September 2019) <www.ft.com/content/93140eac-9cbb-11e9-9c06-a4640c9feebb> accessed 06 October 2020.

King, M, *The End of Alchemy: Money, Banking, and the Future of the Global Economy* (W. W. Norton & Company, 2017).

Knight, B, 'Innovation Will Stall Without a Regulatory Fintech 'Sandbox'', (*American Banker*, 15 November 2016) <https://www.americanbanker.com/opinion/innovation-will-stall-without-a-regulatory-fintech-sandbox> accessed 07 June 2020.

Kenton, W, 'Financial Crisis' (*Investopedia,* 16 March 2020) <www.investopedia.com/terms/f/financial-crisis.asp> accessed 01 November 2020.

Kurzer, R, 'Report: Majority of Companies Fear 3rd-Party Vendors Make Them Vulnerable to GDPR Legal Risks' (*MarTech Today*, 31 July 2018) <https://martechtoday.com/report-majority-of-companies-fear-that-3rd-party-vendors-make-them-vulnerable-to-legal-risks-for-gdpr-non-compliance-218922> accessed 1 August 2020.

Lawrence, A, et al., 'Blockchain and Laws. Are they Compatible?—A White Paper Championed by Baker McKenzie in Collaboration with R3' (*Baker McKenzie*, 2017)

'Learn about Ethereum' (*Ethereum,* 2019) <https://ethereum.org/learn/#ethereum-basics> accessed March 2020.

Lima, C, 'Developing Open and Interoperable DLT/Blockchain Standards' [2018] 51,11, IEEE Computer Society.

Lindsey, N, 'Insurance Not Valid in Case of Cyber War, Says Major Insurance Company' (*Chief Privacy Officer Magazine*, 17 January 2019) <www.cpomagazine.com/cyber-security/cyber-insurance-not-valid-in-case-of-cyber-war-says-major-insurance-company/> accessed 06 March 2020.

Linux Foundation, 'Join the Linux Foundation' (*Linux Foundation*) <www.linuxfoundation.org/membership/join/ > accessed 08 October 2020.

'List of Supervised Banks' (*European Central Bank*) <www.bankingsupervision.europa.eu/banking/list/html/index.en.html> accessed 20 December 2020.

'Live Cyber Threat Map' (*Check Point Software Technologies Ltd,* updated continuously) <https://threatmap.checkpoint.com/> accessed 22 September 2020.

Lloyd's, *Facing the Cyber Risk Challenge: A Report by Lloyd's* (2016).

'Looking into the Crystal Ball: A Report on Emerging Technologies and Security Challenges' (*ENISA,* 2018).

Lucas, R, J Sullivan, J R.C. Nurse, 'Incentivising Cybersecurity through Cyber Insurance' (*Royal United Services Institute*, 2020) <https://rusi.org/projects/incentivising-cybersecurity-through-cyber-insurance> accessed 30 July 2020.

Lyons, Tom and Ludovic Courcelas, 'Blockchain and Cybersecurity' (*EBOF,* 2020).

——, 'Governance of and with Blockchains' (*EBOF,* 2020).

Lyons, Tom, Ludovic Courcelas, and Ken Timsit, 'Blockchain and the GDPR' (*The European Union Blockchain and Observatory Forum,* 2018).

——, 'Legal and Regulatory Framework of Blockchains and Smart Contracts' (*EBOF,* 2019).

——, 'Scalability, Interoperability, and Sustainability of Blockchains' (*The European Union Blockchain and Observatory Forum,* 2019).

Magnus, M, 'Banking Union' (*Factsheets on the European Union: European Parliament,* December 2019) < https://www.europarl.europa.eu/factsheets/en/sheet/88/bnking-union> accessed 20 July 2020.

Malan, D, 'The Law Can't Keep up with New Tech. Here's How to Close the Gap' (*World Economic Forum*, 21 June 2018), <www.weforum.org/agenda/2018/06/law-too-slow-for-new-tech-how-keep-up/> accessed 10 March 2020.

Marinos, L, et al. 'ENISA Threat Landscape Report 2018' (*ENISA*, 2018).

Markopoulou, D, V Papakonstantinou, P d. Hert, 'The New EU Cybersecurity Framework: The NIS Directive, ENISA's role and the General Data Protection Regulation' [2019] *Computer Law & Security Review* 35.

Martin, R, '5 Blockchain Security Risks and How To Reduce Them - Ignite Ltd.' (*Ignite Ltd.*, 2018) <https://igniteoutsourcing.com/blockchain/blockchain-security-vulnerabilities-risks/> accessed 27 February 2020.

McEvoy, E, 'Regulation needs to match the pace of fintech innovation' (*Fintech Bulletin,* 18 May 2020) <https://fintech-bulletin.com/regulation-needs-to-match-the-pace-of-fintech-innovation/> accessed 10 September 2020.

McGuinness, D, 'How a Cyber Attack Transformed Estonia' (*BBC,* 2017) <www.bbc.com/news/39655415> accessed 27 March 2020.

McMillan, R, 'The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster' (*WIRED*, 3 March 2014) <https://www.wired.com/2014/03/bitcoin-exchange/> accessed 27 February 2020.

Michels, D, 'Here's How GDPR and the Blockchain Can Coexist' (*The Next Web*, 26 July 2018) <https://thenextweb.com/syndication/2018/07/26/gdpr-blockchain-cryptocurrency/> accessed 08 October 2020.

Moret, E, and P Pawlak, 'The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime' (*European Union Institute for Security Studies,* 2017).

Moulinos, K, C Karsberg, M.A.C. Dekker, *Proposal for Article 19 Incident Reporting: Proposal for an Incident Reporting Framework for eIDAS Article 19* (*ENISA,* 2015).

Muguruza, B.T., et al., 'Challenges to Effective EU Cybersecurity: Briefing Paper' (*European Court of Auditors*, 2019).

Nakashima, E, 'NSA Found a Dangerous Microsoft Software Flaw and Alerted the Firm—Rather than Weaponizing it' (*The Washington Post*, 14 January 2020) <www.washingtonpost.com/national-security/nsa-found-a-dangerous-microsoft-software-flaw-and-alerted-the-firm--rather-than-weaponize-it/2020/01/14/f024c926-3679-11ea-bb7b-265f4554af6d_story.html> accessed 20 September 2020.

'National Terrorism Risk Insurance Programmes of OECD Countries with Government Participation' (*OECD*, 2016).

'Netherlands (NL)', (*Cyberwiser.eu: Cyber Range and Capacity Building in Cybersecurity,* 2018) <www.cyberwiser.eu/netherlands-nl> accessed 20 April 2020.

Newman, L H, 'The Leaked NSA Spy Tool That Hacked the World' (*Wired,* 7 March 2018) <www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/> accessed 12 June 2020.

——, 'Hacker Lexicon: What are Zero-Knowledge Proofs?' (*Wired*, 14 September 2019) <www.wired.com/story/zero-knowledge-proofs/> accessed 30 September 2020.

Ng, C, 'Regulating Fintech: Addressing Challenges in Cybersecurity and Data Privacy', (*Harvard Kennedy School,* 22 February 2018) <www.innovations.harvard.edu/blog/regulating-fintech-addressing-challenges-cybersecurity-and-data-privacy> accessed 6 June 2020.

'NHS Cyber-Attack: GPs and Hospitals Hit by Ransomware' (*BBC,* 13 May 2017) <https://www.bbc.com/news/health-39899646> accessed 22 March 2020.

'NIS Cooperation Group' (*European Commission*, 24 July 2020) <https://ec.europa.eu/digital-single-market/en/nis-cooperation-group> accessed 01 August 2020.

Norry, A, 'The History of the Mt Gox Hack: Bitcoin's Biggest Heist' (*Blockonomi*, 31 March 2020) <https://blockonomi.com/mt-gox-hack/> accessed 27 February 2020.

'NotPetya' (*Council of Foreign Relations*, July 2017) <www.cfr.org/cyber-operations/notpetya> accessed 20 September 2020.

OECD, *The Role of Cyber Insurance in Risk Management* (OECD Publishing, 2017).

Ogun, M N (ed.), *Terrorist Use of Cyberspace And Cyber Terrorism* (IOS Press 2015).

Orcutt, M, 'How Secure is Blockchain Really?' (*MIT Technology Review*, 25 April 2018) <www.technologyreview.com/2018/04/25/143246/how-secure-is-blockchain-really/> accessed 08 October 2020.

——, 'Once Hailed as Unhackable, Blockchains Are Now Getting Jacked' (*MIT Technology Review*, 19 February 2019) <www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/ > accessed 06 October 2020.

'Organisation & Governance' (*SWIFT*) <https://www.swift.com/about-us/organisation-governance > accessed 08 October 2020.

Olano, G, 'Singapore Launches First Commercial Cyber Risk Pool' (*Insurance Business,* 30 October 2018) <www.insurancebusinessmag.com/asia/news/cyber/singapore-launches-first-commercial-cyber-risk-pool-115040.aspx> accessed 29 April 2020.

Otmar, L, '"National CERT" vs. "National CSIRTs"', (*Computer Emergency Response Team Austria*, 1 August 2018) <https://cert.at/en/blog/2018/8/blog-20180731155524-2252> accessed 30 August 2020.

'Our Approach', (*Belgian Business CIO Forum*) <https://www.cioforum.be/> accessed 1 0May 2020.

Ouzounis, V, 'Good Practice Guide on Reporting Security Incidents' (*ENISA,* 2009).

Panitz, D, and B Gordon, 'Balancing the Equation Between Technology and Effective Legal Project Management' (*Law.com: Corporate Counsel,* 6 March 2020) <https://www.law.com/corpcounsel/2020/03/06/balancing-the-equation-between-technology-and-effective-legal-project-management/?slreturn=20200810110120> accessed 10 September 2020.

Park, K, and S Sen, 'Third-party Governance and Risk Management: The Threats are Real' (*Deloitte,* 2016).

Parlour, R, S Bouyon, S Krause, *Cybersecurity in Finance: Getting the Policy Mix Right!—Report of a CEPS-ECRI Task Force* (Centre for European Policy Studies and European Credit Research Institute, 2018).

Parsons, A, K Simmonds, J Gibbs, 'A Cyber-Attack vs an Act of War: Conflicting Positions in Marriott and Mondelez' (*Womble Bond Dickinson (UK) LLP* and *Lexology*, 31 January 2020) <www.lexology.com/library/detail.aspx?g=dec0f622-5ee6-4de9-8ff2-d6b9e4adaf8c> accessed 22 September 2020.

Ponemon Institute, 'Data Risk in the Third-Party Ecosystem: Third Annual Report' (2018)

Pupillo, L, 'Encouraging Responsible Vulnerabilities Disclosure', (*OECD Global Forum on Digital Security for Prosperity*, 2019).

'REFIT – Making EU Law Simpler, Less Costly and Future Proof' (*European Commission*) <https://ec.europa.eu/info/law/law-making-process/evaluating-and-improving-existing-laws/refit-making-eu-law-simpler-less-costly-and-future-proof_en> accessed 01 November 2020.

'Regulatory Sandboxes', (*Columbia Business School: The Columbia Institute for Tele-information*, 2016) <https://dfsobservatory.com/content/regulatory-sandboxes> accessed 04 June 2020.

'Regulatory Sandboxes and Experimentation Clauses as Tools for Better Regulation: Council Adopts Conclusions' (*European Council*, 16 November 2020), <www.consilium.europa.eu/en/press/press-releases/2020/11/16/regulatory-sandboxes-and-experimentation-clauses-as-tools-for-better-regulation-council-adopts-conclusions/> accessed 16 November 2020.

'Reports', (*EBOF*) <www.eublockchainforum.eu/reports> accessed 22 February 2020.

'Reporting a Cyber Security Incident', (*National Cyber Security Centre UK*) <https://report.ncsc.gov.uk/> accessed 20 April 2020.

Ros, G, 'The Making of a Cyber Crash: A Conceptual Model for Systemic Risk in the Financial Sector' (*ESRB*, 2020).

'Russian Military 'Almost Certainly' Responsible for Destructive 2017 Cyber Attack' (*National Cyber Security Centre, UK,* 14 February 2018) <www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack> accessed 20 September 2020.

Sanchez, I, and L Beslay, 'EU Zero-Day Vulnerability Management: Challenges and Opportunities to Improve The Security and Resilience of the Digital Single Market', presentation at the CEPS Workshop on Software Vulnerability Disclosure: The European Landscape (Brussels, 23 June 2017).

Schaake, M, L Pupillo, A Ferreira, G Varisco, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges—Report of a CEPS Task Force* (CEPS, 2018)

'Shaping Europe's digital future' (*European Commission*) <https://ec.europa.eu/digital-single-market/en> accessed 29 April 2020.

'Shared Vision, Common Action: A Stronger Europe—A Global Strategy for the European Union's Foreign and Security Policy' (*European Union External Action Service*, 2016).

Shooter, S, 'Cyber Insurance: Debunking the myths' (*Bird & Bird LLP* and *Lexicology*, 28 June 2019) <www.lexology.com/library/detail.aspx?g=26cddd55-b7ab-495d-b832-afc4a37fcac1> accessed 24 September 2020.

Silfversten, E, W Phillips, G.P. Paoli, C Ciobanu, *Economics of Vulnerability Disclosure* (*ENISA,* 2018).

Simpson, A, 'Enhancing the Digital Economy Through Collaboration on Vulnerability Research Disclosure' (*National Telecommunications and Information Administration, United States Department of Commerce,* 09 July 2015) <www.ntia.doc.gov/blog/2015/enhancing-digital-economy-through-collaboration-vulnerability-research-disclosure> accessed 11 March 2020.

'Single Supervisory Mechanism' (*European Central Bank*) <www.bankingsupervision.europa.eu/about/thessm/html/index.en.html> accessed 20 September 2020.

Skinner, C, 'Will the Blockchain Replace Swift?' (*American Banker*, 08 March 2016) <www.americanbanker.com/opinion/will-the-blockchain-replace-swift> accessed 30 September 2020.

Smith, B, 'The Need for Urgent Collective Action to Keep People Safe Online: Lesson's From Last Week's Attack' (*Microsoft,* 14 May 2017) accessed 1 August 2020.

'Statement from the Press Secretary' (*The White House*, 15 February 2018) <www.whitehouse.gov/briefings-statements/statement-press-secretary-25/> accessed 20 September 2020.

Stolton, S, "We are a Prime Target,' Schinas says, as Commission Strives to Bolster Cyber Resilience' (*Euractiv*, 16 December 2020) <www.euractiv.com/section/cybersecurity/news/we-are-a-prime-target-schinas-says-as-commission-strives-to-bolster-cyber-resilience/> accessed 16 December 2020.

Stubbings, T, et al., 'Complying with the European NIS Directive: Cybersecurity for Critical Infrastructures' (*KPMG,* 2019).

Stupp, C, 'Ansip: Member States Will Need Help from EU Cyber Emergency Fund' (*Euractiv,* 14 September 2017) <https://www.euractiv.com/section/cybersecurity/news/ansip-member-states-will-need-help-from-eu-cyber-emergency-fund/> accessed 23 September 2020.

'SWIFT on Distributed Ledger Technologies: Delivering an Industry-Standard Platform through Community Collaboration' (*SWIFT & Accenture,* 2016).

'SWIFT talks about XRP – Hong Kong Blockchain Week!' (*CNBC Africa*, 11 March 2019) <https://youtu.be/xS36_foCEQ4?t=863> accessed 30 September 2020.

Tasca, P and Tomaso A, 'Crypto Assets and the Regulator's Role: Ignore, Regulate or Kill?' (*Open Access Government,* 18 July 2018) <//www.openaccessgovernment.org/crypto-assets-and-the-regulators-role-ignore-regulate-or-kill/47858/ > accessed 08 October 2020.

Taurins, E, 'EU MS Incident Response Development Status Report' (*ENISA*, 2019).

Taylor, A, *Credit, Financial Stability, and the Macroeconomy* (National Bureau of Economic Research, 2015).

'Testing Cooperation of EU CSIRTs Network during Large-Scale Cyber-Attacks' (*ENISA,* 16 May 2019) <https://www.enisa.europa.eu/news/enisa-news/testing-cooperation-of-eu-csirts-network-during-large-scale-cyber-attacks> accessed 21 October 2020.

'The Anatomy of a 51% Attack and How You Can Prevent One' (*Komodo*, 2018) <https://komodoplatform.com/51-attack-how-komodo-can-help-prevent-one/> accessed 27 February 2020.

'The Data Controller and Data Controller Duties under the GDPR' (*i-SCOOP*) <www.i-scoop.eu/gdpr/data-controller-data-controller-duties/> accessed 18 September 2020.

'The EU's Cybersecurity Strategy for the Digital Decade' (*European Commission*, 16 December 2020) <https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade> accessed 18 December 2020.

'The European Blockchain Services Infrastructure is on its Way' (*CEF Digital*, 25 September 2019) <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/09/25/The+European+Blockchain+Services+Infrastructure+is+on+its+way> accessed 06 October 2020.

'The First Cohort of the First Fintech Regulatory Sandbox' (*BBVA*, 28 May 2018) <www.bbva.com/en/first-cohort-first-fintech-regulatory-sandbox/> accessed 01 September 2020.

'The NIS Directive' (*Cyberwatching.eu*) <https://cyberwatching.eu/policy-landscape/cybersecurity/nis-directive-and-its-challenges> accessed 21 October 2020.

'The Privileged Access Threat Report 2019' (*BeyondTrust*, 2019) <www.beyondtrust.com/resources/whitepapers/privileged-access-threat-report> accessed 5 May 2020.

'The Tasks of the Single Contact Point (German abbreviation "ZASt")' (*Federal Commissioner for Data Protection and Freedom of Information*) <https://www.bfdi.bund.de/ZASt/EN/ENZAST/ZAST_Artikel/Aufgaben_ZASt.html> accessed 10 September 2020.

Thomas, L.G., 'The Case for Federal Regulatory Sandbox for FinTech Companies' [2018], *N.C. Banking Inst.* 22..

'Tiber-EU Framework: How to Implement the European Framework for Threat Intelligence-Based Ethical Red Teaming' (*European Central Bank*, 2018).

'Transaction Rate Per Second' (*Blockchain*) <www.blockchain.com/charts/transactions-per-second> accessed 20 December 2020.

Van der Burg, S, 'Co-shaping the Life Story of a Technology: From Technological Ancestry to Visions of the Future' in Simone van der Burg and Tsjalling Swierstra (eds), *Ethics on the Laboratory Floor* (Palgrave Macmillan, 2013).

Van Pelt, R, et al., 'Defining Blockchain Governance: A Framework for Analysis and Comparison', (Information Systems Management, 2020).

Verizon 2019 'Data Breach Investigations Report' [not open access] quoted in Judy Selby and Peter McLaughlin, 'Is Insurance Coverage for Cyber Claims Barred by War Exclusion?' (*20iapp*, 25 June 2019), <https://iapp.org/news/a/setting-the-record-straight-on-cyberinsurance-claim-denials-and-the-war-exclusion/> accessed 03 March 2020.

Vermaak, W, 'MiCA: A Guide to the EU's Proposed Markets in Crypto-Assets Regulation' (*Sygna,* 23 November 2020) <www.sygna.io/blog/what-is-mica-markets-in-crypto-assets-eu-regulation-guide/> accessed 27 December 2020.

Véron, N, *Europe's Radical Banking Union* (Bruegel, 2015).

Vigna, P, '5 Things About Mt. Gox's Crisis' (*The Wall Street Journal*, 25 February 2014) <https://blogs.wsj.com/five-things/2014/02/25/5-things-about-mt-goxs-crisis/> accessed 27 February 2020.

'Virtual Currencies Key Definitions and Potential AML/CFT Risks' (*Financial Action Task Force*, 2014).

'Vulnerability Scan in Kaspersky Total Security' (*Kaspersky*) <https://support.kaspersky.com/11474 > accessed 20 September 2020.

Werbach, K, *The Blockchain and the New Architecture of Trust* (MIT Press, 2018).

Westby, J, 'Why the EU is About to Seize the Global Lead on Cybersecurity' (*Forbes Magazine,* 31 October 2019)

<https://www.forbes.com/sites/jodywestby/2019/10/31/why-the-eu-is-about-to-seize-the-global-lead-on-cybersecurity/#4b6b78d72938> accessed 20 September 2020.

'What are 'Controllers' and 'Processors'?' (*Information Commissioner's Office*) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/> accessed 18 September 2020.

'What is the Common Backstop' (*European Stability Mechanism*, 2020) <www.esm.europa.eu/content/what-common-backstop-0> accessed 08 December 2020.

'What is a Data Controller or a Data Processor?' (*European Commission*) <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en> accessed 16 December 2020.

'What is Hybrid CoE?: The European Centre of Excellence for Countering Hybrid Threats' (*Hybrid CoE*) <www.hybridcoe.fi/> accessed 19 September 2020.

'What is the Banking Union?', (*European Commission*) <https://ec.europa.eu/info/business-economy-euro/banking-and-finance/banking-union/what-banking-union_en> accessed 20 April 2020.

'What is the Single Resolution Fund?' (*Single Resolution Board*) <https://srb.europa.eu/en/content/single-resolution-fund> accessed 27 March 2020.

'What Makes a Bank Significant?' (*European Central Bank*) <www.bankingsupervision.europa.eu/banking/list/criteria/html/index.en.html> accessed 27 December 2020.

'What Responsibilities and Liabilities Do Controllers Have When Using a Processor?' (*Information Commissioner's Office*, 2019) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/responsibilities-and-liabilities-for-controllers-using-a-processor/> accessed 27 February 2020.

'What We Do' (*NSS Labs*) <www.nsslabs.com/tested-technologies/threat-detection-analytics-tda/> accessed 20 September 2020.

'When Protection is Key' (*Depositors Insurance Fund*) <www.difxs.com/DIF/Home.aspx>, accessed 20 September 2020.

Woolich, A, F Burling, J Kelly, 'All Change—Are You Compliant with the EU General Data Protection Regulation?: Special Update', (*Holman Fenwick Willan LLP,* September 2018).

Wright, T, 'Ethereum Now Rivals bitcoin for Daily Value Transfers' (*Cointelegraph*, 16 April 2020) <https://cointelegraph.com/news/ethereum-now-rivals-bitcoin-for-daily-value-transfers> accessed 10 September 2020.

Wu, M, 'Third Party Vendor Breaches Still Major Cybersecurity Issue' (*SecurityScorecard*, 20 July 2016) <https://securityscorecard.com/blog/third-party-vendor-breaches-2016-1> accessed 27 February 2020.

'Zero-day Vulnerability: What it is, and How it Works' (*Norton*) <https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html> accessed 10 March 2020.

APPENDIX

The following sections provide further information on incident reporting frameworks, emerging technologies, and legal grey-zones mentioned in the body of the paper.

i. ENISA's Template Guidelines for Two-Stage eIDAS Incident Reporting

ENISA's proposals for incident reporting stages and template content are as follows:[702]

'When it comes to notifying authorities, it is very common that the providers of a service adopt a two-phase approach. According to this, the provider submits an initial and short description of the incident to the supervisory body and then, at a later stage, when details of the incident have been identified, he/she provides a more detailed and descriptive notification. Information collected from an incident notification might include:'

'First incident notification'

- 'Date and time the security incident detected (or started if known already)'
- 'Contact details: contact details for questions about this security incident'
- 'Provider concerned: name of the company'
- 'Trust service(s) impacted (or potentially impacted): description of the service(s)'
- 'Personal data impacted (or potentially impacted): description of the personal data impacted'
- 'Short description of the security incident'
- 'Measures taken or planned: summarise what measures are taken or planned'
- 'Cross-border impact'

'Final incident notification'

- 'Date and time the security incident started'
- 'Date and time the security incident detected by the [trust service provider]'
- 'Contact details: contact details for questions about this security incident'
- 'Provider concerned: name of the company'
- 'Trust service(s) impacted: description of the service(s)'
- 'Security feature(s) affected: confidentiality, integrity, availability etc'.

[702] *Article 19 Incident reporting: Incident reporting framework for eIDAS Article 19* (ENISA, 2016) 31.

- 'Personal data impacted: description of the personal data impacted'
- 'Number of customers affected'
- 'Duration of the incident'
- 'Root cause category: One of human errors, malicious actions, natural disaster or system failure'
- 'Detailed cause of the security breach'
- 'Detailed assets affected'
- 'General description of the security incident: For example, affected IT-systems, how was the incident detected, how long the incident was active, is there a vulnerability in a software which involves a third party etc.'
- 'Cost estimation'
- 'Measures taken: summarize what measures were taken to mitigate the incident'
- 'Long term measures, taken or plan, to avoid similar incidents from happening in the future'
- 'Cross-border impact'
- 'Other authorities notified'
- 'Customers affected notified'
- 'Public informed'

ii. UK's NCSC Incident Reporting Template

The UK's NCSC incident reporting form asks for:[703]

- 'What organisation are you reporting for?'
- 'Which sector is the organisation in?'
- 'What is your role?'
- 'Summary of incident'
- 'Are you sharing this with us for information or do you require advice and assistance?'
- 'Do you have an internal ID for the incident?'
- 'Investigation so far'

[703] 'Reporting a cyber security incident' (*National Cyber Security Centre, UK*) <https://report.ncsc.gov.uk/> accessed 20 April 2020. Contains public sector information licensed under the Open Government Licence v3.0.: www.nationalarchives.gov.uk/doc/open-government-licence/version/3/.

- 'Impact (none, minor, moderate, major, catastrophic, not yet known)'
- 'Description of impact'
- 'Current state of incident (reported/newly discovered, ongoing investigation containment achieved, restoration achieved, incident remediated)'
- 'Who else has been notified'
- 'Have you reported this to the Information Commissioner's Office (ICO) as a GDPR obligation?'
- 'Have you reported this to the relevant Competent Authority (CA) as a NIS Directive obligation?'
- 'Do you have any further data or samples to aid this incident?'

iii. Singapore's Incident Reporting Template for the Financial Sector

The Monetary Authority of Singapore's template can serve as a model with respect to the degree of specificity it requests for reports about incidents impacting financial institutions.[704] It takes a multi-stage reporting approach, for which reporters are prompted for a large range of sector-specific and technical details in the first instance. Later reports use the same template to send updates on any given field. There are additional prompts for the final reporting stage, once an analysis of the incident as a whole can be conducted.

iv. Mt. Gox Incident

The events that brought down Mt. Gox are a cautionary tale to those who are overly confident regarding the extent of blockchain's security. Mt. Gox was a Japanese bitcoin exchange that at its peak saw 70% of all bitcoin transactions pass through its systems, before a major hack caused it to fold.[705] It remains unclear whether the hack was an inside job or perpetrated by external actors.[706]

[704] 'Incident Reporting Template' (*Monetary Authority of Singapore,* 21 June 2013) <www.mas.gov.sg/regulation/forms-and-templates/incident-reporting-template> accessed 10 March 2020.
[705] Mehmet Nesip Ogun (ed.), *Terrorist Use of Cyberspace and Cyber Terrorism* (IOS Press 2015); Paul Vigna, '5 Things About Mt. Gox's Crisis' (*The Wall Street Journal*, 25 February 2014) <https://blogs.wsj.com/five-things/2014/02/25/5-things-about-mt-goxs-crisis/> accessed 27 February 2020; Marius-Christian Frunza, *Solving Modern Crime In Financial Markets* (Academic Press 2015).
[706] Andrew Norry, 'The History of the Mt Gox Hack: Bitcoin's Biggest Heist' (*Blockonomi*, 31 March 2020) <https://blockonomi.com/mt-gox-hack/> accessed 27 February 2020.

The lead-up to Mt. Gox's fall began in 2011, when its private key was compromised.[707] The criminals were able to access and steal bitcoins from the exchange undetected over several years.[708] In total they siphoned off 740,000 BTC, valued at almost €460 million at the time.[709]

According to insiders, the company had poor software management practices and did not have adequate cybersecurity measures in place.[710] With languishing technical bugs that were not addressed promptly, the firm's weaknesses in these respects undermined consumers' confidence.[711] This was seen in the 36% decline in BTC's value, despite its sound cryptographic fundamentals not being directly compromised.[712]

The story of Mt. Gox's fall serves as a cautionary tale for those who overestimate blockchain technology's high security, since its fall indicates that the surrounding technical infrastructure required to support a distributed ledger can remain vulnerable to cyber incidents. Blockchain should thus not be misconstrued as a silver bullet against current cybersecurity threats, for the age-old adage that 'a chain is only as strong as its weakest link' is likely to hold true.

As discussed in Sections III.V. and IV.V., key issues to consider regarding the implementation of blockchain in the financial sector include establishing common technical standards and compatibility with privacy-related regulation and anti-money laundering laws, the latter of which conflicts with many public blockchains' principle of anonymity. In addition, integration with or replacement of legacy systems pose security issues at the time of cryptocurrency transfers. More developed processes and standards are required to improve interoperability between blockchains and with legacy infrastructures in order to mitigate the risks that arise from conducting system transfers at scale.

v. Ethereum Hack and Hardforking

The Ethereum hack exemplifies the challenges of determining who to hold accountable and what constitutes appropriate interventions in public blockchains. Should the miners, code developers, or someone/thing else be held responsible? Particularly in imperfectly decentralised systems, to what extent should intervention play a role in enforcing regulations?

---

[707] Andrew Norry, 'The History of the Mt Gox Hack: Bitcoin's Biggest Heist' (*Blockonomi*, 31 March 2020) <https://blockonomi.com/mt-gox-hack/> accessed 27 February 2020.
[708] ibid.
[709] ibid.
[710] Robert McMillan, 'The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster' (*WIRED*, 3 March 2014) <www.wired.com/2014/03/bitcoin-exchange/> accessed 27 February 2020.
[711] Michael Ashton, *What's Wrong With Money? The Biggest Bubble Of All* (John Wiley & Sons, 2016)
[712] ibid.

In the space of public and open blockchains, Ethereum can be considered the next evolution step after Bitcoin.[713] Bitcoin lacks the ability of a generalised computation, which Ethereum enables by introducing the notion of smart contracts.[714] Smart contracts are programming that simulate a business logic on blockchains.[715]

In 2016, an ambitious smart contract called the Decentralised Autonomous Organisation (DAO) was launched by Ethereum. This implemented the logic of venture capitalism. The DAO enabled investors to invest their funds in the form of Ether (the underlying cryptocurrency of Ethereum) to fund start-up projects of their choosing. The project managed to raise $100 million worth of Ether within a timeframe of less than a month.

However, there was a logical fallacy in the source code of the DAO which enabled hackers to steal $70 million worth of Ether. The Ethereum organisation intervened by hardforking the underlying financial records and reimbursing those whose funds were stolen. Hardforking is the act of starting a new chain of records and thereby invalidating the old transaction data. A few in the community went against this move, as they were of the view that it went against blockchain's basis of immutable and decentralised record keeping. The dissenters chose to continue on the pre-hardfork system and named it Ethereum Classic.

Due consideration must be given to how such hacks should be handled in future, especially since the problem of identifying controllers remains an issue in the industry more widely.

vi. 51% Attacks

Blockchain platforms where mining power is concentrated in the hands of fewer nodes allow nodes that form a majority to override past transactions.[716] Such concentrated mining power means that it is even more important that each node functions properly.[717] If control of the blockchain is restricted to a smaller number of nodes, each node controls a larger percentage of the hashing power in the system than do nodes on more decentralised blockchains.[718] Consequently, more concentrated blockchain platforms are more vulnerable to concerted cyber

[713] Klint Finley, 'A $50 Million Hack Just Showed That the DAO Was All Too Human' (*Wired,* 18 June 2016) <https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/> accessed 10 March 2020.
[714] 'Learn about Ethereum' (*Ethereum,* 2019) <https://ethereum.org/learn/#ethereum-basics> accessed March 2020.
[715] ibid.
[716] Jake Frankenfield, '51% Attack', (*Investopedia,* 2019) <www.investopedia.com/terms/1/51-attack.asp> accessed 29 February 2020.
[717] ibid.
[718] ibid.

incidents.[719] With each node holding a greater percentage of the information in the system, a few compromised nodes can put large amounts of data at risk.[720] Malicious actors would have to overcome the defences of fewer nodes to control 51% of the system's hashing power.[721] Attackers that are able to seize control of the majority of nodes (i.e., 51% or more) have the power to disrupt and dominate transactions.[722] They can manipulate subsequent transaction records to hide the use of coins that they then use more than once.[723]

vii. Categorising Financial Threats to Blockchain

Name	Impact	Incidents	Solutions	Link to financial sector	Ref.
Crypto-currency money laundering	On decentralised ledgers accounts may not be linked to a personal identity; bitcoin tumblers can be used to launder money	2.5 billion USD is estimated to have been laundered to date e.g. Binance hack	AML (anti money laundering) KYC (know your customer) procedures Shutting down bitcoin tumblers like Europol shutting down BestMixer.io	Unlikely to be a serious threat as all transactions are visible and many exchanges have AML procedures	724
Ransomware	Blackmailing and downtime of key digital infrastructure	2017 Wannacry: users transfer bitcoin to a bitcoin wallet 1/3 of NHS trusts affected	Having a service provider who can identify bitcoin addresses associated with ransomware	Cryptocurrency (based on blockchain) is used as an anonymous way to collect payments Loss of data	725
Cryptojacking	Usage of users' computational resources to mine cryptocurrency without consent	Coinhive injected into websites intentionally or through hijacking (Pirate Bay using it as an alternate revenue source)	User consent and opt out; extensions like ad blockers; anti-virus software	Fake websites links confusing users; financial firms moving to cloud services which can be hijacked	726

[719] Jake Frankenfield, '51% Attack', (*Investopedia,* 2019) <www.investopedia.com/terms/1/51-attack.asp> accessed 29 February 2020.
[720] ibid.
[721] ibid.
[722] ibid.
[723] ibid.
[724] 'Cryptocurrency Anti-Money Laundering Report 2018' (*Ciphertrace.com*, 2018) <https://ciphertrace.com/crypto-aml-report-2018q3.> accessed 27 February 2020.
[725] Andy Greenberg, 'Hold North Korea Accountable for Wannacry—And The NSA, Too' (*Wired*, 19 December 2017) <https://www.wired.com/story/korea-accountable-wannacry-nsa-eternal-blue/?fbclid=IwAR2Uq1_VRe7XjhTCrmIcq6KYWN88ChNrn4UzoxfpOLDNfmWUB_EU_LEjngs> accessed 27 February 2020.
[726] 'Cryptojacking - Cryptomining In the Browser' (*ENISA,* 10 November 2017). <https://www.enisa.europa.eu/publications/info-notes/cryptojacking-cryptomining-in-the-browser?fbclid=IwAR0h32Ir23DAyp0RLYO_hiGgTiNpmkQ21V1gjK3IESKsTreQKvy9xRIbndE> accessed 27 February 2020.

51% attacks	Altering past records and manipulation State actors can launch attacks on permission-less ledger	Ethereum Classic (ETC) successfully hit by attack in 2019	There is security software available (e.g., Komodo) which punishes parallel forks or by locking in existing blocks	Websites (e.g., NiceHash, MiningRig Rentals) can be rented to launch attacks Transaction records can be wiped out; double spending occurs	727
End-point attacks	Leakage of private key causing data leak (attack on end-users and vendors)	Mt. Gox's auditor account with admin rights was hacked	Conventional security protocols	Not adopting 3rd party blockchain.	728
Teething issues	All of the above	DAO code on Ethereum was attacked and 55mil was lost through double spending Bitomat lost 17k BTC during a server reboot as it accidentally lost keys to all BTC wallets	Rigorously testing code before releasing it	Risk of vulnerabilities when system is built and continually updated over time. If a cloud provider like AWS is attacked all data can be lost if not backed up	729
DDoS attacks	Disrupted service	DDoS attacks on blockchain nodes will reduce performance	Have multiple nodes to continue running the system	An attack may target all banks with nodes from the same blockchain ledger	730

[727] 'The Anatomy of a 51% Attack and How You Can Prevent One' (*Komodo*, 2018) <https://komodoplatform.com/51-attack-how-komodo-can-help-prevent-one/> accessed 27 February 2020; 'Cost of a 51% Attack for Different Cryptocurrencies | Crypto51' (*Crypto51.app*, 2020) <www.crypto51.app/> accessed 27 February 2020.

[728] R Martin, '5 Blockchain Security Risks and How To Reduce Them - Ignite Ltd.' (*Ignite Ltd.*, 2018) <https://igniteoutsourcing.com/blockchain/blockchain-security-vulnerabilities-risks/> accessed 27 February 2020.

[729] ibid.

[730] Alexandre Francois, 'Is Blockchain the Perfect Defense Against DDos Attacks?' (*PenTest Magazine*, 25 September 2019) <https://pentestmag.com/is-blockchain-the-perfect-defense-against-ddos-attacks/> accessed 27 February 2020.