Journal of Financial Regulation, 2020, 00, 1–11
doi: 10.1093/jfr/fjaa006
Advance Access Publication Date: 04 August 2020
Panorama

Hybrid and Cyber Security Threats and the EU's Financial System

Maria Demertzis*, and Guntram Wolff**

ABSTRACT

Increasing cyber and hybrid risks will test the European Union's system of fragmentation on issues of security, but centralization on financial and other economic issues. This asymmetry was not an obstacle in a world in which security threats were more contained or of a different nature. But the world is changing. In this article, we document the rise in cyber attacks in the EU. Meanwhile, hybrid threats are real, though difficult to quantify. We then explore preparations to increase the resilience of the financial system in terms of regulation, testing, and governance. We find that at the individual institutional level, significant measures have been taken, even though there are diverging views on whether individual companies are sufficiently prepared. More worryingly, preparations appear less advanced at the system-wide level. We recommend that EU finance ministers increase resilience through regular preparedness exercises and greater consideration of system-wide regulatory issues. A broader political discussion on the integration of the EU security architecture applicable to the financial system should also be advanced. This includes reopening the framework on foreign-investment screening in order to have screening of foreign investment in critical financial infrastructure at the EU level.

KEYWORDS: cyber security; financial stability; financial regulation; EU legislation; hybrid threats

I. INTRODUCTION

'Fantasia' is a Member State of the European Union and the euro area. Fantasia's finance minister is woken at midnight by her chief of staff alerting her to social media reports showing documents that implicate her in illegal pre-election financing. While she knows this is not true, she spends much of the rest of the night mobilizing experts to prove that the documents posted on the internet are false. But the citizens of Fantasia, who dislike

* Maria Demertzis, Deputy Director, Bruegel, Rue de la Charité 33, 1210 Saint-Josse-ten-Noode, Belgium; maria.demertzis@bruegel.org

** Guntram Wolff, Director, Bruegel, Rue de la Charité 33, 1210 Saint-Josse-ten-Noode, Belgium; guntram.wolff@bruegel.org. This article benefitted from numerous interviews the authors have carried out with senior European and national policymakers and executives from the financial sector. We have also benefitted from feedback from Zsolt Darvas, Stephen Gardner, André Sapir, Thomas Wieser, and Nicolas Véron on an earlier draft, and excellent research assistance by Catarina Midoes, Jan Mazza, and Kyra Whitelaw. All errors and omissions remain ours.

the minister for her austerity policies, are suspicious of the ministry's early morning press statement. Trust in the government is falling.

Early next morning, on her way to the first meeting of the day, the minister is informed that the biggest bank in the country has faced a run. It started with messages on Facebook, Twitter, and Instagram reporting that the bank's cash dispensers do not work, and showing citizens queuing outside various branches unable to withdraw money from their accounts. The bank's CEO immediately issues a public statement that an unfounded social media smearing campaign is taking place and follows the appropriate emergency protocol: informing the board, the bank's domestic supervisor, and the supervisor in Frankfurt, and putting crisis-management teams in place. However, despite the CEO's best efforts, panicked citizens rush to withdraw their savings. The bank, the minister is informed, is now out of cash and requires additional liquidity as soon as possible.

An electricity blackout in the capital increases confusion, while simultaneously the internet slows down across the entire country—there seems to be a connectivity problem. Citizens in Fantasia's neighbouring country begin to worry—after all, the bank has major subsidiaries in their country too and the public sector has no information on what is happening in Fantasia. The government of Fantasia's neighbour calls the EU's Hybrid Fusion Cell in the European External Action Service (EEAS), which collects and analyses evidence from such cases. However, the EEAS has received little information from Fantasia. Meanwhile, Fantasia's finance minister issues a statement that domestic deposits are protected by a guarantee and tries to reassure citizens that the government will honour all claims and protect citizens against malicious attacks. What happens next?

Several events occurring at the same time, as described in this scenario, would constitute a hybrid attack. Because of the nature of the attack involving diverse, simultaneous incidents, players in the corporate and political worlds would find it difficult to see the whole picture. Situation analysis and awareness of the degree of interconnectedness are key to better understanding. Political judgement, necessary to contain the fallout from such attacks in real time, needs to be able to rely on well-established procedures based on thorough analytical evidence and knowledge.

The example simulates a reality for which preparations need to be made, especially in the light of recent individual attacks. In 2007 Estonia experienced something that comes perhaps closest to our Fantasia example.[1] In 2014, Bulgarian banks experienced a run, triggered by an 'attack' when an unsigned news bulletin spread via social media.[2] Electricity blackouts can affect entire countries (as recently seen in Argentina, Uruguay,

1 DamienMcGuinness, 'How a cyber attack transformed Estonia' BBC (27 April 2017) <https://www.bbc.com/news/39655415> accessed 3 June 2020.

2 Andrew McDowall, 'Second Bulgarian bank faces run as pressure on system builds' Financial Times (27 June 2014) <https://www.ft.com/content/40692919-312a-39e0-acd4-bce8c899ac66> accessed 3 June 2020; Leonid Bershidsky, 'Bulgaria's a Soft Target for Bank Runs' Bloomberg (2 July 2014) <https://www.bloomberg.com/opinion/articles/2014-07-01/bulgaria-s-a-soft-target-for-bank-runs> accessed 3 June 2020; Silvia Merler, 'Fact of the week: A spam newsletter caused a bank run in Bulgaria' Bruegel (2 July 2014) <https://bruegel.org/2014/07/fact-of-the-week-a-spam-newsletter-caused-a-bank-run-in-bulgaria/> accessed 3 June 2020.

and Paraguay)[3] and can be caused by cyber attacks, as happened with the December 2015 Kiev power outage.[4] Social media attacks against politicians are a well-studied area.[5] Meanwhile, a slowdown of the internet can be caused by physical or cyber attacks against the internet infrastructure, including deep-sea cables, on which a lot of the internet traffic depends.[6]

The European Union considers hybrid 'activities by State and non-state actors' to 'pose a serious and acute threat to the EU and its Member States'.[7] According to the European Commission and the High Representative:

efforts to destabilise countries by undermining public trust in government institutions and by challenging the core values of societies have become more common. Our societies face a serious challenge from those who seek to damage the EU and its Member States, from cyber attacks disrupting the economy and public services, through targeted disinformation campaigns to hostile military actions.[8]

2. CYBER ATTACKS ARE AN INCREASING, AND INCREASINGLY COSTLY, RISK

The frequency and cost of cyber attacks have increased. According to a report by Hiscox, 61 per cent of companies they surveyed reported one or more cyber events in 2018, up from 45 per cent the previous year and the cost of those attacks is rising.[9] The reported average loss increased 61 per cent from 2018 to 2019, reaching $369,000. The report surveyed 5,400 firms in the US, UK, Belgium, France, Germany, Spain, and the Netherlands. Approximately three out of four businesses failed a cyber-readiness test. Also, the report notes many cyber incidents involve viruses/worms, which might not constitute an 'attack' on a specific company.[10] The 2019 *SonicWall Cyber Threat Report* found over the course of 2018 an escalation in the volume of cyber attacks and new, targeted threat tactics used by cyber criminals.[11] The Verizon *2019 Data Breach Investigations Report* found that financial motives were the main reason for data

3 'Argentina, Uruguay, Paraguay suffer massive power blackout' *Deutsche Welle* (16 June 2019) <https://www.dw.com/en/argentina-uruguay-paraguay-suffer-massive-power-blackout/a-49225070> accessed 3 June 2020; Lewis Sanders, 'How Argentina's nationwide blackout happened' *Deutsche Welle* (17 June 2019) <https://www.dw.com/en/how-argentinas-nationwide-blackout-happened/a-49232203> accessed 3 June 2020.

4 Pavel Polityuk, Oleg Vukmanovic and Stephen Jewkes, 'Ukraine's power outage was a cyber attack: Ukrenergo' *Reuters* (18 January 2017) <https://www.reuters.com/article/us-ukraine-cyberattack-energy/ukraines-power-outage-was-a-cyber> attack-ukrenergo-idUSKBN1521BA> accessed 3 June 2020.

5 Wu He, 'A review of social media security risks and mitigation' (2012) JournalofSystemsandInformationTechnology>.

6 Rishi Sunak, *Undersea Cables* (Policy Exchange 2017) <https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf> accessed 3 June 2020.

7 Commission, 'Increasing resilience and bolstering capabilities to address hybrid threats', Joint Communication to the European Parliament, the European Council and the Council, JOIN (2018) 16 final.

8 Ibid.

9 Hiscox, *Hiscox Cyber Readiness Report 2019* (7 December 2018) <https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf> accessed 3 June 2020.

10 Ibid.

11 SonicWall, *2019 SonicWall Cyber Threat Report* (26 March 2019) <https://www.sonicwall.com/resources/white-papers/2019-sonicwall-cyber-threat-report/> accessed 3 June 2020.

breach attacks, but espionage was behind 25 per cent of attacks.[12] Data breaches arising from attacks often remain undetected for a considerable period of time. There is also evidence that small and medium-sized companies are often targets of attacks. The German industry association BITKOM estimated that in 2016–17, German companies incurred damage of €43 billion from data espionage and sabotage. Seven out of 10 manufacturing companies have been subject to attacks according to BITKOM.[13] By contrast, a report published in 2019 by the UK government Department for Digital, Culture, Media and Sport showed that 32 per cent of businesses had identified a cyber-security attack in the previous 12 months, down from 43 per cent the previous year.[14]

Figure 1 documents the number of cyber incidents experienced by listed companies each year in Europe as reported in the press. While media reports capture only a fraction of the actual incidents, there is a clear upward trend in incidents affecting financial companies.

Cyber attacks are not restricted to listed companies but are also relevant for public and other institutions. Given the highly interconnected nature of our economic systems, an attack on a public sector entity might well have repercussions for the financial system (for example, 5 million Bulgarians had their personal data stolen in an attack on the Bulgarian tax authority in mid-2019).[15]

The literature on the impact of terrorism on the financial system can help discern some of the implications of physical-infrastructure disruptions related to attacks. Large-scale terror attacks can disrupt physical infrastructure, as can hybrid attacks in which, for example, deep-sea cables are targeted. It is therefore useful to look at the empirical literature assessing the impact of events such as the 11 September 2001 (9/11) attacks. The literature typically finds that even a large and successful terror attack such as 9/11 does not fundamentally endanger the stability of the global financial system or the global economy more broadly. While specific sectors such as the airline and defence industry might see lasting changes to their valuations,[16] the market as a whole recovered relatively quickly.[17] Longer-term major fiscal and human costs resulted from the US

12 Verizon, *2019 Data Breach Investigations Report* (8 May 2019) <https://enterprise.verizon.com/resources/reports/dbir/> accessed 3 June 2020.

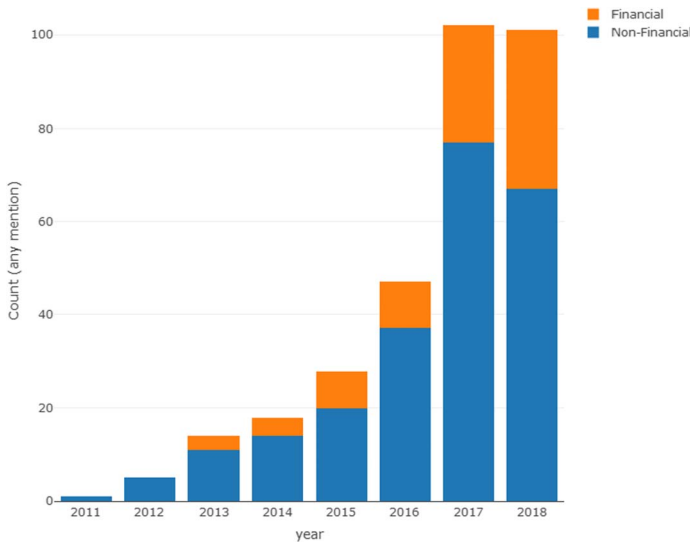
13 Christoph Krösmann and Teresa Ritter, 'Attacks on German industry caused 43 billion euros in damage' *Bitkom* (13 September 2018) <https://www.bitkom.org/Presse/Presseinformation/Attacken-auf-deutsche-Industrie-verursachten-43-Milliarden-Euro-Schaden.html> accessed 3 June 2020.

14 Department for Digital, Culture, Media and Sport, *Cyber Security Breaches Survey 2019* (3 April 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf> accessed 3 June 2020.

15 Marc Santora, '5 Million Bulgarians Have Their Personal Data Stolen in Hack' *New York Times* (17 July 2019) <https://www.nytimes.com/2019/07/17/world/europe/bulgaria-hack-cyberattack.html?searchResultPosition=3> accessed 3 June 2020.

16 Konstantinos Drakos, 'Terrorism-induced structural shifts in financial risk: airline stocks in the aftermath of the September 11th terror attacks' (2004) 20 European Journal of Political Economy 435; Dirk Brounen and Jeroen Derwall, 'The Impact of Terrorist Attacks on International Stock Markets' (2010) 16 European Financial Management 585; Emmanuel Apergis and Nicholas Apergis, 'The 11/13 Paris terrorist attacks and stock prices: the case of the international defense industry' (2016) 17 Finance Research Letters 186.

17 Andrew Chen and Thomas Siems, 'The effects of terrorism on global capital markets' (2003) 20 European Journal of Political Economy 349; Jussi Nikkinen and Sami Vähämaa, 'Terrorism and stock market sentiment'



Source: Bruegel. Note: We classify articles in Factiva as *cyber-attack news*if they contain the words 'Cyber attack', while simultaneously falling into any of the Factiva classifications 'Malware', 'Data breaches' or 'Cybercrime/Hacking' (Factiva articles in 31 languages).Factiva also identifies by name the company being discussed in these articles. One or more cyber-attack articles written about a listed company in any given month counts as one 'cyber-attack event'. A 'cyber-attack event' might not necessarily correspond to an actual cyber attack but, for example, to new measures companies take to fight cyber attacks, among other issues.

Figure 1. Number of 'cyber-attack events' affecting listed companies domiciled in the EU-28 countries, including the financial and non-financial sectors, as reported by the media.

response to 9/11 in the form of wars.[18] But for the financial system alone, the rapid recovery observed was due to significant redundancy systems and to decisive policy action in the form of additional central bank liquidity and effective communication.[19]

III. AN EVOLVING LANDSCAPE FOR MANAGING CYBER SECURITY AND HYBRID THREATS TO THE FINANCIAL SYSTEM

The EU has responded to hybrid threats with an extensive set of policies. The European Union Institute for Security Studies provides a good summary of hybrid threats and the respective policy responses.[20] They find substantial shortcomings such as inadequate information sharing and intelligence exchange (including with EU institutions), and

(2010) 45 Financial Review 263; Bertrand Maillet and Thierry Michel, 'The impact of the 9/11 events on the American and French stock markets' (2005) 13 Review of International Economics 597; Timothy Burch, Douglas Emery and Michael Fuerst, 'What can "nine-eleven" tell us about closed-end fund discounts and investor sentiment?' (2010) 38 The Financial Review 515.

18 B Frey, S Luechinger and A Stutzer, 'Calculating tragedy: Assessing the costs of terrorism' (2007) 21 Journal of Economic Surveys 1.

19 Chen and Siems (n 17); Robert Johnston and Oana Nedelescu, 'The impact of terrorism on financial markets' (2006) 12 Journal of Financial Crime 7; Daniel Fiott and Roderick Parkes, 'Protecting Europe: the EU's response to hybrid threats' (April 2019) European Union Institute for Security Studies (EUISS) Chaillot Paper 151.

20 Fiott and Parkes (ibid).

risk assessments that are based on the lowest common denominator among Member States, suboptimal collaboration with the private sector, and compartmentalization of EU institutions. Official communications on hybrid threats make little reference to the financial system's vulnerability to hybrid threats. The financial system, however, is considered an essential service by the Network and Information Security Directive,[21] under which EU countries must supervise the cyber security of such critical market operators (energy, transport, water, health, and finance sector) in their territories.

Cyber risks are typically managed as part of a financial institution's traditional operational risk management framework. This framework is insufficient. The European Central Bank (ECB) sets out four key reasons why it falls short of what is needed.[22] A distinguishing characteristic of cyber attacks is often the persistent nature of a campaign conducted by a motivated attacker. As a result, cyber attacks are often difficult to identify and fully eradicate, and they can have a substantial impact. Second, cyber risks posed by an interconnected entity are not necessarily related to the degree of the entity's relevance to a financial institution's business. Third, cyber attacks can render some risk-management and business-continuity arrangements ineffective. Fourth, cyber attacks can be stealthy and propagate rapidly. We would add a fifth point: cyber attacks can be systemic if they exploit shared vulnerabilities. These could, for example, result from a limited number of companies providing cyber security to major financial institutions, leading to similar cyber-protection systems and vulnerabilities in several institutions.

To increase resilience against hybrid and cyber attacks against the financial system, the EU has taken a three-part approach: (i) regulations and standards; (ii) testing and preparedness; (iii) governance.

Attempts to promote cyber security, including for financial market infrastructures (FMIs), have led to a number of initiatives at all levels: globally, at EU level and at national level. At the global level, the G7 Cyber Expert Group first took steps in 2013 to develop a set of high-level (but non-binding) fundamental principles for assessing the level of cyber security. The EU adopted a cyber-security strategy in the same year. The EU finalized the Network and Information Security Directive in 2016—an initiative taken to tackle the cyber-security challenges in a coordinated attempt. When it comes to the financial sector in particular, the European Banking Authority, the Committee on Payments and Market Infrastructures, and the International Organization of Securities Commissions have taken a number of initiatives.

The European Central Bank's governing council adopted cyber-resilience oversight expectations (CROE) for the Eurosystem in 2018.[23] CROE is structured in a way that outlines expectations on governance, identification and detection of cyber risks, protection, testing, and putting in place procedures for response and recovery. Concrete measures aim to promote coordination and standardization in two areas: identifying

21 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, (2016) OJ L 194/1.

22 ECB, *Cyber resilience oversight expectations for financial market infrastructures* (December 2018).

23 Ibid.

weak parts of the system (*testing*), and ensuring that business continues following a breach (*quick recovery*).

The ECB, in line with international institutions such as the Bank for International Settlements, has formulated clear expectations on how governance at the level of the individual financial institution should be structured. For example, the ECB discussed in detail the expectation that board and management should have an awareness culture and also clear procedures involving large parts of the organization on how to deal with a cyber attack in real time.[24] We do not have systematic evidence on how well these expectations have been implemented in individual institutions but surveys suggest that the awareness and preparedness of individual institutions has increased. Surveys from ACCA,[25] Kaspersky[26] and TD Ameritrade Institutional[27] show that cyber security is increasingly being prioritized by companies. Cyber-security service providers are also expanding in revenue and achieving record product sales, while large technology companies, including BlackBerry, Symantec, IBM, BAE Systems, and CISCO, are redirecting their investments towards cyber security.[28]

A more worrying aspect is the governance set-up to manage cyber and hybrid threats at a more systemic level. A key concern we have identified, in our interviews in particular, relates to the institutional interplay between private firms and European and national authorities. In the EU, security questions are dealt with by and large by national authorities, while the single market is a true EU endeavour. This asymmetry of governance is becoming problematic as the global security environment becomes less benign. As trust in the US providing for European security declines,[29] this asymmetry becomes an obstacle to effective cyber security.

IV. ADVANCING THE EU'S FINANCIAL RESILIENCE TO HYBRID AND CYBER RISKS

The risks to the EU's financial system of hybrid and cyber risks are real but difficult to assess. The fact that so far there has not been a major incident with significant systemic repercussions does not mean that there will not be in the future. In the course of our interviews with senior policymakers and private-sector representatives, we explored how they assess the state of play when it comes to regulation, testing, and governance at the level of the institution and at a more systemic level. While necessarily subjective, we have distilled our discussions and reading of public documents into five broad messages:

(i) *There have been significant advances to protect individual institutions.* Considerably less has been done to address the issue from a system-wide perspective. In general,

24 Ibid.

25 ACCA (Association of Chartered Certified Accounts), *Cyber and the CFO Report* (30 May 2019).

26 Kaspersky, *What it takes to be a CISO: The report* (25 October 2018).

27 TD Ameritrade Institutional, *RIA (Registered Investment Advisors) 2019 Sentiment Survey Report* (8 January 2019).

28 Kaspersky (n 26); ACCA (n 25); TD Ameritrade Institutional (n 27).

29 M Leonard, J Pisani-Ferry, E Ribakova, J Shapiro and G Wolff, 'Redefining Europe's economic sovereignty' Policy Contribution No 9, Bruegel (25 June 2019) <https://www.bruegel.org/2019/06/redefining-europes-economic-sovereignty/> accessed 3 June 2020.

Table 1. A heat-map of the EU financial system's preparedness in the face of hybrid and cyber risks

	Regulation	**Testing**	**Governance**
Individual Monetary Financial Institutions (MFIs)	What does regulation on cyber security say? Need to review the liquidity buffers? Need to review the capital requirements?	Are individual MFIs doing enough testing of their vulnerabilities?	Board-level priority, recommendations but how good is implementation?
Financial system	Systemic regulation? Macro-prudential discussion?	G7 exercise has been carried out, no EU exercise to date.	Integrated market but not integrated security structures. ECB and other EU financial supervisors lack counterpart on security side. Capacity to organize rapid macro-policy response.

Green - reasonably prepared
Red - reasonably prepared
(*in sources*: Bruegel assessment based on interviews and reading of publicly available literature).

senior officials are well aware of regulatory, testing, and governance measures recommended for, or required of, individual institutions. The private financial sector, for its part, is alert to cyber-security issues. Many institutions have put in place strong technical and procedural measures to protect their business, but we cannot be sure about the level of preparedness across all companies. But neither policy officials nor the private sector have advanced significantly on the broader systemic dimension. Interlocutors were much less clear when it came to the system as a whole—the perspective that is most relevant when thinking about actual hybrid attacks on a key infrastructure or systemic institutions. Table 1 maps the vulnerabilities based on our interviews and reading of the publicly available material across the three main areas: regulation, testing, and governance in terms of individual institutions and the financial system as a whole.

(ii) *Starting with individual institutions, two issues deserve more deliberation.* First, the joint advice from the European Supervisory Authorities is to streamline existing regulations and guidelines on cyber security.[30] It is not always easy for countries with different legal systems to build a single or coordinated regulatory framework for cyber

30 European Supervisory Authorities, 'Joint advice on the costs and benefits of developing a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector' JC 2019 25 (10 April 2019) <https://eba.europa.eu/documents/10180/2551996/JC+2019+25+%28Joint+ESAs+Advice+on+a+coherent+cyber+resilience+testing+framework%29.pdf> accessed 3 June 2020.

risks. BIS surveyed the range of practices in different jurisdictions in terms of managing cyber risks.[31] They argue that, as the financial sector becomes increasingly digital, greater alignment of national regulation is necessary.[32] Currently, much is done through non-binding guidelines. The CROE example for payment systems points to the lack of regulatory alignment between the ECB and national authorities. We also found little evidence that existing rules on liquidity and capital regulatory requirements treat cyber risks differently to other operational risks that might require the built-up of separate buffers. Second, when it comes to testing and governance, our impression is that large financial companies are actively engaged. But smaller financial and public institutions look less prepared. Unlike typical financial shocks that transmit via large institutions, cyber shocks can transmit as effectively via small institutions.

(iii) *At the level of the system as a whole, significant issues deserve more deliberation.* We received few indications that systemic regulatory questions have been considered. The macro-prudential implications of cyber risks is also a topic that has not received much attention, despite an acknowledgement that cyber risks, let alone hybrid risks, cannot be treated as normal operational risks.

(iv) *Cyber security is ultimately a matter for (and part of) national security in all countries, irrespective of the sector.* National security authorities are informed and ultimately in charge, and security cooperation remains limited in the EU. This will have an impact on the way that cyber security is dealt with in the financial sector, despite banking union and, in the future, Capital Markets Union. This level of complexity is a lot more difficult to deal with as the EU remains still a union of 27 sovereign states.

(v) *The mismatch between strong financial integration and limited security integration could be a cause of systemic weakness.* Strong financial integration means that many key financial services are provided by a limited number of companies that might be concentrated in only a few EU Member States. While the supervision of such systemic institutions is centralized at European level (or there is a high level of supervisory coordination depending on the sector), the institutions' counterparts for security questions are national. This mismatch could lead to systemic weaknesses if national authorities fail to internalize the financial effects that cyber attacks on local financial firms may have beyond national borders.

V. THE WAY FORWARD

The five messages we have outlined indicate that policy discussion on cyber risks should address the following issues:

(i) *Information sharing can be improved within and between jurisdictions.* The Basel Committee reports that most jurisdictions have put in place cyber security information-sharing mechanisms (either mandatory or voluntary) involving banks, regulators, and security agencies.[33] Following an attack, financial institutions are required to report to the authorities. By contrast, there is typically much less communication from the

31 BIS (Basel Committee on Banking Supervision), 'Cyber-resilience: Range of practices' (4 December 2018).
32 Ibid.
33 Ibid.

regulator back to banks, or between regulators across borders. Some EU banks have indicated to us that they receive very little communication from authorities on cyber risks.

(ii) *When it comes to testing, the EU, and the euro area in particular, should consider holding regular preparedness exercises for the financial system.* The G7 under the French presidency undertook a cyber-attack exercise in summer 2019, but to our knowledge no such exercises for the financial system have been carried out at the EU or euro-area level. Clear assignment of responsibilities and rapid cross-border collaboration between national and European authorities and the private sector are critical to understanding how to reduce the damage and recover quickly. While ENISA carries out exercises in other sectors,[34] an EU-wide exercise focusing on the financial system seems warranted.

(iii) *The tension between national sovereignty on security matters and shared responsibility for financial-system stability creates multiple challenges.* For example, responses to cyber incidents involve law-enforcement agencies, which do not necessarily follow a sufficiently integrated approach to account for the wider implications to the EU financial system. Even more difficult is the question of political judgement and response to hybrid threats. Who analyses such risks and threats in real time from a truly EU-wide perspective? ENISA, the European Union Agency for Cybersecurity, and the Hybrid Fusion Cell at the EEAS are useful institutional bases for a more systemic and EU-wide response. But both ENISA and the Hybrid Fusion Cell are institutionally rather small with limited mandates and capacity to analyse and react in real time. EU institutions themselves can become victims of cyber and hybrid attacks. While the institutions have obviously put in place significant measures to protect themselves, the question is whether sufficient public sector security infrastructure can be provided to them, including at the political level. How quickly would the EU be capable of defining a political response to a successful cyber attack on, say, the ECB? It is a big endeavour to improve and upgrade the coordination of national security agencies and EU capacity at the level of shared institutions. However, we believe it is imperative in such a highly integrated financial system. An alternative would be to reduce financial integration with a view to reducing the scope of spillover from cyber and hybrid threats onto the financial system.[35] However, this option would be inconsistent with a highly integrated financial system at the core of a monetary union and an integrated single market.

(iv) *The issue of ownership of critical infrastructure, for example ownership of a stock exchange, a systemically important bank or even mobile networks, is left to EU Member States.* But if subject to cyber attacks, their ramifications could be felt across the EU financial system. The point here is not to say that foreign ownership is the problem; rather that a national sovereign decision can have significant implications for the entire EU financial system. The current EU investment screening framework is insufficient.

(v) *A more integrated and better-functioning insurance market for cyber risks can help manage the costs but also help the competent authorities understand the risks.* The insurance market against cyber risks is relatively small and suffers disproportionately from the

34 See <www.cyber-europe.eu>.

35 Joseph E Stiglitz, 'Risk and Global Architecture: Why Full Financial Integration May Be Undesirable' (May 2010) 100 American Economic Review: Papers & Proceedings 388.

problems any insurance market suffers from (information asymmetry, adverse selection). In the EU, the issue is compounded by the lack of a central security authority and information sharing. Yet, creating the right conditions for an insurance market to develop can help in two ways. First, the ability to insure against cyber risks will help cushion the cost for any individual entity that comes under attack. Second, allowing for a market, and therefore a pricing system, to develop will help understand the extent and gravity of these risks. Defining a methodology that is common across the EU could be an important contribution to the creation of an EU-wide insurance market. Also, creating uniform information and disclosure requirements would be a useful step forward.

(vi) *The response to a major systemic cyber or hybrid incident might also require a swift and decisive macro policy response.* As we noted in section II, the initial policy reaction to the 9/11 terror attacks involved significant liquidity provisioning. Evidence suggests that this immediate and sizable response reduced the impact on the American economy.[36] The EU should be aware of this and be ready to act in a timely manner.

As cyber and hybrid risks increase, the EU's system of fragmentation on issues of security, but centralization on financial and other economic issues, will be tested. This asymmetry was not an obstacle in a world in which security threats were more contained (or of a different nature) and the EU trusted the United States to be its security guarantor. We believe that Europe will be increasingly asked to provide for its own security, and as a unit. At the very least, it will require a greater level of collaboration among national authorities.

36 International Monetary Fund (IMF), World Economic Outlook—The Global Economy after September 11 (December 2001).