Demertzis, Maria; Wolff, Guntram B.

Research Report

Hybrid and cybersecurity threats and the European Union's financial system

Bruegel Policy Contribution, No. 2019/10

Provided in Cooperation with:
Bruegel, Brussels

Suggested Citation: Demertzis, Maria; Wolff, Guntram B. (2019) : Hybrid and cybersecurity threats and the European Union's financial system, Bruegel Policy Contribution, No. 2019/10, Bruegel, Brussels

This Version is available at:
https://hdl.handle.net/10419/237635

Policy Contribution
Issue n°10 | September 2019

Hybrid and cybersecurity threats and the European Union's financial system

Maria Demertzis and Guntram Wolff

MARIA DEMERTZIS (maria.demertis@bruegel.org) is Deputy Director of Bruegel

GUNTRAM WOLFF (guntram.wolff@bruegel.org) is Director of Bruegel

This Policy Contribution was prepared for the informal meeting of EU economic and financial affairs ministers (Ecofin) in Helsinki, 13-14 September 2019. The paper benefitted from numerous interviews the authors carried out with senior European and national policymakers and executives from the financial sector. We 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.

Executive summary

INCREASING CYBER AND HYBRID risks will test the European Union's system of fragmentation on issues of security but centralisation 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.

WE DOCUMENT THE RISE in cyber attacks in the European Union. Meanwhile, hybrid threats, involving conventional and non-conventional means, are real, though difficult to quantify. We 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 of the financial system through regular preparedness exercises and greater consideration of system-wide regulatory issues. We also consider it necessary to advance a broader political discussion on the integration of the EU security architecture applicable to the financial system. This includes reopening the framework on foreign-investment screening in order to ensure screening of foreign investment in critical financial infrastructure at the EU level.

bruegel

1 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 mobilising experts to prove that the documents posted on the internet are false. But citizens, who in any case dislike 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 issues immediately a public statement that there is an unfounded social media smearing campaign against his bank and follows the appropriate emergency protocol: informing the board, the domestic supervisor and the supervisor in Frankfurt, and putting crisis-management teams in place. However, despite the CEO's best efforts, citizens stricken by panic rush to withdraw their savings. The bank, the minister is informed, is now out of cash and requires liquidity as soon as possible.

An electricity blackout in the capital increases confusion while in the meantime the internet in the entire country slows down – 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. Fantasia's neighbour government 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 assure citizens that the government will honour all claims and protect citizens against malicious attacks. What happens next?

Such events occurring simultaneously 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 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 or recent individual attacks. Estonia in 2007 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 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 subject (He, 2012; de Boer *et al*, 2012). Meanwhile, a slowdown of the internet can be caused by physical or cyber attacks against the

1 See for example https://www.bbc.com/news/39655415.

2 See https://www.bloomberg.com/opinion/articles/2014-07-01/bulgaria-s-a-soft-target-for-bank-runs, https://www.ft.com/content/40692919-312a-39e0-acd4-bce8c899ac66 and https://bruegel.org/2014/07/fact-of-the-week-a-spam-newsletter-caused-a-bank-run-in-bulgaria/.

3 See https://www.dw.com/en/argentina-uruguay-paraguay-suffer-massive-power-blackout/a-49225070 and https://www.dw.com/en/how-argentinas-nationwide-blackout-happened/a-49232203.

4 See https://www.reuters.com/article/us-ukraine-cyber attack-energy/ukraines-power-outage-was-a-cyber attack-ukrenergo-idUSKBN1521BA.

internet infrastructure, including against deep-sea cables, on which a lot of the internet traffic depends (Sunak, 2017).

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***"** (European Commission/High Representative, 2018)**.** According to European Commission/High Representative (2018), *"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."* The EU understands hybrid threads and campaigns to be *"multidimensional, combining coercive and subversive measures, using both conventional and unconventional tools and tactics (diplomatic, military, economic, and technological) to destabilise the adversary. They are designed to be difficult to detect or attribute, and can be used by both state and non-state actors"* (European Commission/High Representative, 2018).

Cyber attacks, meanwhile, can be part of a hybrid attack but not every cyber attack is a hybrid threat. Companies, institutions and governments can be victims of such attacks. Financial companies face significant risks of cyber attacks unrelated to any hybrid tactics, which might be motivated purely by criminal reasons. Conversely, hybrid attacks, even if not targeted at the financial system, can have huge repercussions for the financial system, for example as malware spreads.

2 Cyber attacks are an increasing, and increasingly costly, risk

The frequency and cost of cyber attacks have increased. Sixty-one percent of companies reported one or more cyber event in 2018, up from 45 percent the previous year and the cost of those attacks is rising (Hiscox, 2019)[5]. The 2019 *SonicWall Cyber Threat Report* finds over the course of 2018 an escalation in the volume of cyber attacks and new, targeted threat tactics used by cyber criminals (SonicWall, 2019). The Verizon 2019 data breach investigations report found that financial motives were the main reason for data breach attacks, but espionage was behind 25 percent of attacks (Verizon, 2019). 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[6]. By contrast, the UK government Department for Digital, Culture, Media and Sport (DCMS, 2019) showed that 32 percent of businesses had identified a cyber security attack in the last 12 months, down from 43 percent the previous year. DCMS (2019) ascribed this reduction partly to new cybersecurity measures taken by companies in response to the introduction of tough new data privacy laws under the UK Data Protection Act and the EU General Data Protection Regulation.

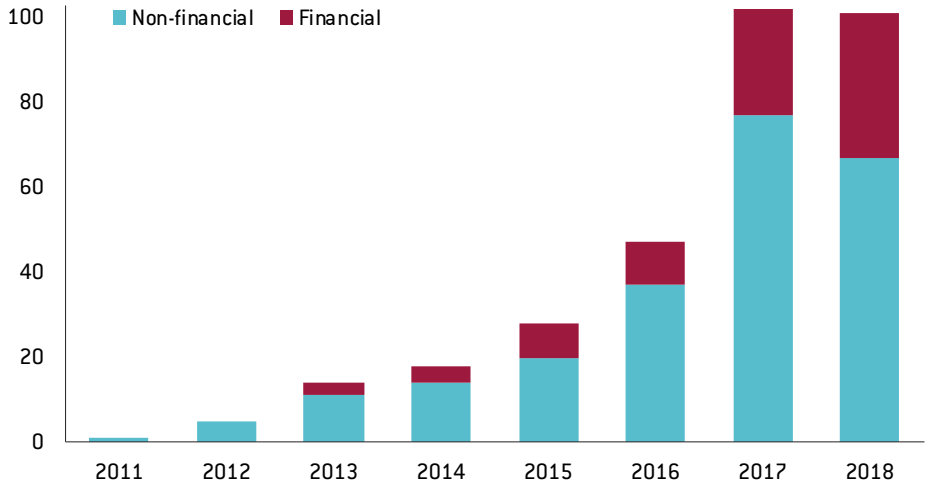
Figure 1 documents the number of cyber incidents experienced by listed companies each

5 The reported average loss increased 61 percent from 2018 to 2019, reaching $369,000 (Hiscox, 2019). 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. However, Hiscox (2019) notes many cyber incidents involve viruses/worms, which might not constitute an 'attack' on a specific company.

6 https://www.bitkom.org/Presse/Presseinformation/Attacken-auf-deutsche-Industrie-verursachten-43-Milliarden-Euro-Schaden.html.

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. In an empirical exercise, we show that the effects of cyber attacks on a company's value can be significant (see the Annex).

Figure 1: Number of 'cyber-attack events' affecting listed companies domiciled in the EU28, financial and non-financial sector, as reported by the media



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.

Given the highly interconnected nature of our economic systems, a cyber attack on a public sector entity can have repercussions for the financial system

Cyber attacks are not restricted to listed companies but are also relevant for public and other institutions. Figure 2 lists the various EU28 institutions reported in the press as having been subject to notable cyber attacks in the past 12 months. Again, while press reports cover only a fraction of actual attacks, it is evident that the issue concerns a broad range of entities across sectors and topics. 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, five million Bulgarians had their personal data stolen in an attack on the Bulgarian tax authority in mid-2019[7]. This data could potentially represent risks to financial firms if, for example, stolen identities are used by criminals. The scope and complexity of modern economic systems imply that the downside risks of cyber attacks can be extremely disruptive and costly.

The literature on the impact of terrorism on the financial system can help discern some of the implications of physical-infrastructure disruptions related to hybrid 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 attacks in the United States on the companies concerned and on the stability of the financial system, in order to better understand the effects of physical disruptions to infrastructure. Theoretically, three impacts can be distinguished: the short-term market impact arising from the destruction of value; the medium-term confidence effects and the longer-term effects on productivity. The empirical 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

7 See for example https://www.nytimes.com/2019/07/17/world/europe/bulgaria-hack-cyberattack.html?searchResultPosition=3.

economy more broadly. While specific sectors such as the airline and defence industry might see lasting changes to their valuations[8], the market as a whole recovered relatively quickly[9]. Longer-term major fiscal and human costs resulted from the US response to 9/11 in the form of wars (Frey *et al*, 2007). But for the financial system alone, the rapid recovery observed was due to significant redundancy systems, such as back-up systems in different cities, at the company level and at the systemic/institutional level, and to decisive policy action in the form of additional central bank liquidity and effective communication[10].

Figure 2: Notable cyber attacks in the EU28 in the year to July 2019 as reported in the press

Source: Bruegel based on Factiva and CSIS data. Note: Cyber attacks were identified through a Factiva search for *cyber-attack news* published between August 2018 and July 2019 (as explained in the note to Figure 1). We identified additional attacks through the 'Significant Cyber Incidents' list provided by the Center for Strategic & International Studies (CSIS), which focuses on "*cyber attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars*"[11].

8 See Drakos (2004), Brounen and Derwall (2010) and Apergis and Apergis (2016).
9 See Chen and Siems (2003), Nikkinen and Vahamaa (2010), Maillet and Michel (2005) and Burch and Emery (2003).
10 See Chen and Siems (2003), Johnston and Nedelescu (2006) and Ferguson (2003).
11 Available at https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

3 An evolving landscape for managing cybersecurity and hybrid threats to the financial system

The EU has responded to hybrid threats with an extensive set of policies. There is no single definition of hybrid threats but most definitions include conventional and non-conventional aggression by state and/or non-state actors. The European Union Institute for Security Studies provides a good summary of hybrid threats and the respective policy responses (Fiott and Parkes, 2019). They find substantial shortcomings such as inadequate information sharing and intelligence exchange (including with EU institutions), and risk assessments that are based on the lowest common denominator among member states, which could lead to underestimation of risks. They also highlight that collaboration with the private sector is suboptimal and that EU institutions find it difficult to overcome compartmentalisation when devising strategies and responses to hybrid threats. They argue that the real challenge for the EU is to recognise and respond to a 'staccato' of events based on credible intelligence coupled with good political judgement. Official communications on hybrid threats make little specific 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 (NIS Directive, 2016/1148/EU), under which EU countries must supervise the cybersecurity 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, but this is insufficient

Cyber risks are typically managed as part of a financial institution's traditional operational risk management framework. This framework is insufficient. ECB (2018) sets out four key reasons why it falls short of what is needed. 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 to fully eradicate and they can have a substantial impact. Second, and moreover, 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. In other words, unlike in traditional financial contagion, a small business partner might pose as big a risk to a given firm as a major partner. 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 scarcity of cybersecurity providers 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 cybersecurity, 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 cybersecurity. The EU adopted a cybersecurity strategy in the same year. The EU finalised the NIS Directive in 2016, an initiative taken to tackle the cybersecurity 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 Organisation of Securities Commissions have taken a number of initiatives to mitigate ICT risks and provide for information security.

The European Central Bank's governing council adopted cyber-resilience oversight expectations (CROE) for the Eurosystem in 2018 (ECB, 2018)[12]. 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. It has three key purposes: 1) provide FMIs with detailed steps on how to operationalise the guidance given; 2) provide a framework to those who oversee FMIs for evaluating the level of cybersecurity; and 3) provide a basis for a communication between FMIs and their supervisors. Concrete measures aim at promoting coordination and standardisation in two areas: identifying weak parts of the system – *testing,* and ensuring business continuing following a breach – *quick recovery*.

European financial regulators are increasing their efforts to promote good testing practices. The ECB sets expectations in CROE in terms of what constitutes a good testing framework[13]. At the same time the European Supervisory Authorities issued advice on how to provide a coherent framework across the EU, including on which parts of existing regulations will need to be adjusted (ESAs, 2019). The EU has now produced a testing framework called TIBER-EU that was developed jointly by the ECB and the European System of Central Banks, and is based on the results of earlier similar testing frameworks including the UK's CBEST and the Dutch TIBER-NL. Such tests are typically voluntary and focus mostly on penetration vulnerabilities. Increasingly, there are tests that focus on the recovery capabilities of entities. TIBER-EU therefore is there to provide a framework for improving resilience rather than for holding entities to account.

CROE expectations all set a target to recover essential services within a two-hour period, following a cyber attack. All available guidance emphasises the need for availability and continuity of critical services. This involves setting targets in terms of both the minimum level of services that should remain available, and the time frame for recovery. While the aim is to restore critical services within a two-hour period, full recovery should be expected by the end of the day of the disruption, in particular for functions that are systemically relevant.

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, ECB (2018) discussed in detail that board and management should have an awareness culture and also clear procedures involving large parts of the organisation to be able to deal with a cyber attack in real time. 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[14].

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

12 This followed on from various initiatives. The European Banking Authority (EBA) published a set of guidelines on ICT risk assessment in 2017, supplementing its own general Supervisory Review and Evaluation Process guidelines, which are used when the supervisor evaluates whether a bank meets capital requirements and manages risks. These guidelines refer to measures to mitigate ICT risks, information security and recommend that measures be put in place. The Committee on Payments and Market Infrastructures and the International Organisation of Securities Commissions published guidance on cyber resilience for all FMIs in 2016, complementing its own Principles for Financial Market Infrastructures.

13 The ECB also emphasises the need for dynamism in approaching cybersecurity (Kopp *et al*, 2017). This requires promoting situational awareness and a process of continuous learning as cyber-related threats change and evolve.

14 Surveys from ACCA (2019), Kaspersky (2018) and TD Ameritrade Institutional (2019) show that cybersecurity is increasingly being prioritised by companies. Cybersecurity 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 cybersecurity.

problematic as the global security environment becomes less benign. At the same time, the EU relies on the US for a military guarantee and vital elements of the security infrastructure. As trust in the US declines and security weaknesses become apparent (Leonard *et al*, 2019), this asymmetry becomes an obstacle to effective cyber security.

The supervisory infrastructure of the EU's financial system has obviously evolved substantially in the last decade, with a much greater degree of centralisation and coordination, in particular because of the Single Supervisory Mechanism at the ECB and the European Supervisory Authorities (ESA). There has not been, however, a corresponding increase in institutional collaboration, let alone centralisation of the security infrastructure[15]. The intelligence sharing between national security institutions and EU institutions or national institutions of other countries is sub-optimal according to analysts (Fiott and Parkes, 2019) and the EEAS calls on member states to increase intelligence sharing between national services and the EEAS-based service in charge of assembling and analysing hybrid threats (the Hybrid Fusion Cell)[16].

4 Reinforcing 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. Risks to the financial system from hybrid threats are multifaceted and do not originate necessarily in the financial system itself. Critical financial and other infrastructures need to be part of a strategy against hybrid threats. It is therefore important that the EU strengthens its resilience.

It is difficult to assess how adequately prepared the EU is to address these risks. 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:

1. **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, 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 cybersecurity 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[17]. It is our understanding that 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

15 The European Centre of Excellence for countering Hybrid Threats in Helsinki is an intergovernmental think tank, also supported by NATO and the EU. Other institutions with primarily analytical capacities exist, such as the European Union Institute for Security Studies.

16 See https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf.

17 There are conflicting messages here. When we spoke to large individual financial firms, they were confident that they take adequate cybersecurity measures. However, a survey run by IMD International (Switzerland, World Competitiveness Center, www.imd.org/wcc) showed that business leaders in many countries increasingly believe that cybersecurity is not adequately addressed. Also there are strong theoretical arguments why individual institutions might underinvest in cybersecurity, as they have an incentive to capitalise on other firms' actions (Gordon *et al*, 2015).

the three main areas: regulation, testing and governance in terms of individual institutions and the financial system as a whole.

2. **Starting with individual institutions, two issues deserve more deliberation. First**, the joint advice from the European Supervisory Authorities (ESAs, 2019) is to streamline existing regulations and guidelines on cybersecurity. It is not always easy for countries with different legal systems to build a single or coordinated regulatory framework for cyber risks[18]. 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 very actively engaged. But it is less clear if smaller financial institutions and public institutions are similarly prepared. Unlike typical financial shocks that transmit via large institutions, cyber shocks might transmit as effectively via small institutions.
3. **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 macroprudential 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.

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

	Regulation	Testing	Governance
Individual FMI	What does regulation on cybersecurity 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, but no EU exercise. Euro-area exercise?	Integrated market but not integrated security structures. ECB and other EU financial supervisors lack counterpart on security side. Capacity to organise rapid macro-policy response

Source: Authors' assessment based on interviews and reading of publicly available literature.

18 BIS (2018) surveyed the range of practices in different jurisdictions in terms of managing cyber risks. They found that most regulators have taken action to promote the creation of frameworks that enhance the cyber resilience of those they regulate. They did that by either issuing principles-based guidance or prescriptive regulation. The Basel Committee commented on the lack of homogeneity in approach, style and regulatory requirements across the globe. And while most regulatory authorities expect entities to have a cybersecurity strategy, they do not actually require it. As the financial sector is becomes increasingly digital there is a need for greater alignment of national regulatory and supervisors.

4. **Cybersecurity 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 cybersecurity 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 28 sovereign states.
5. **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 member states. While the supervision of such systemic institutions is centralised 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 internalise the financial effects that cyber attacks on local financial firms can have beyond national borders. Similarly, a cyber attack on the electricity or water supply system of an EU state could harm financial firms' activities, domestically and abroad.

5 The way forward?

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

1. **Information sharing can be improved within and between jurisdictions.** The Basel Committee (BIS, 2018) reports that most jurisdictions have put in place cyber-security information-sharing mechanisms (either mandatory or voluntary) involving banks, regulators and security agencies. Following an attack, financial institutions are required to report to the authorities. BIS (2018) also found that banks communicate adequately between themselves, with the regulator and with national security agencies in the event of an attack. By contrast, there is typically much less communication going from the 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, in contrast to the detailed information banks are required to provide. Collaboration between the private sector and public authorities is important when it comes to information exchange and responding to ongoing attacks**,** as also emphasised by the NIS Directive**.**
2. **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 in summer 2019 a cyber-attack exercise, 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 the European Union Cybersecurity Agency (ENISA) carries out exercises in other sectors[19], an EU-wide exercise focusing on the financial system seems warranted.
3. **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

The tension between national sovereignty on security matters and shared responsibility for financial-system stability creates multiple challenges.

19 See www.cyber-europe.eu.

How quickly would the EU be capable of defining a political response to a cyber attack on, say, the European Central Bank?

threats. Who analyses such risks and threats in real time from a truly EU-wide perspective? ENISA and the EEAS Hybrid Fusion Cell are useful institutional bases for a more systemic and EU wide response[20]. 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? **Some progress in strengthening the mandate and competence of EU-level security agencies was made recently but this cannot be the endpoint given the high degree of interconnectedness.** 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[21].

4. **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**. To the extent that ownership has implications for management decisions and board procedures, foreign ownership of an important financial infrastructure could have implications for financial resilience against cyber attacks. On 14 February 2019, the European Parliament adopted an EU framework for screening foreign direct investment (Regulation (EU) 2019/452). This law[22] introduces a mechanism for cooperation and information-sharing among member states but stops short of giving veto powers to the Commission. The objective of the framework is greater coordination on national security-related screening of foreign investment. It will help increase awareness and increase peer pressure across the EU. But it does not establish an independent EU authority for investment screening and also falls short of a single EU framework for assessing security risks. We consider the new framework to be a step in the right direction but ultimately not commensurate with the challenge created by an integrated single market and still essentially national screenings of investments for national security reasons. 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.
5. **A more integrated and better-functioning insurance market for cyber risks can help manage the costs but also help understand the risks themselves.** The insurance market against cyber risks is relatively small and suffers disproportionally from the 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 for a pricing system, to develop will help understand the extent and gravity of these risks. Helping therefore to define 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 will be a helpful step forward.
6. **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 2, the initial policy reaction

20 See for example EPRS (2019).

21 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 (see Stiglitz, 2010, for a theoretical exposition of the argument for limiting integration). However, this option would be inconsistent with a highly integrated financial system at the core of a monetary union and an integrated single market.

22 See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0452.

to the 9/11 terror attacks involved significant liquidity provisioning by the Fed. Evidence suggests that this immediate and sizable response reduced the impact on the American economy[23]. 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 centralisation 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.

References

ACCA (2019) *Cyber and the CFO*, Association of Chartered Certified Accountants

Apergis, E. and N. Apergis (2016) 'The 11/13 Paris terrorist attacks and stock prices: the case of the international defense industry', *Finance Research Letters* 17 (C): 186-192

Arcuri, M.C., M. Brogi and G. Gandolfi (2017) 'How does cybercrime affect firms? The effect of information security breaches on stock returns', Proceedings of the First Italian Conference on Cybersecurity, January

BIS (2018) *Cyber-resilience: Range of practices,* Basel Committee on Banking Supervision, December

Brounen, D. and J. Derwall (2010) 'The Impact of Terrorist Attacks on International Stock Markets', *European Financial Management* 16 (4): 585-598

Burch T., D. Emery and M. Fuerst (2010) 'What can "nine-eleven" tell us about closed-end fund discounts and investor sentiment?' *The Financial Review* 38: 515-529

Chen, A. and T. Siems (2003) 'The effects of terrorism on global capital markets', *European Journal of Political Economy* 20 (2): 349-366

DCMS (2019) *Cyber Security Breaches Survey 2019,* UK Department for Digital, Culture, Media & Sport, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf

de Boer, N., H. Sütfeld and J. Groshek (2012) 'Social media and personal attacks: A comparative perspective on co-creation and political advertising in presidential campaigns on YouTube', *First Monday* 17(12)

Drakos, K. (2004) 'Terrorism-induced structural shifts in financial risk: airline stocks in the aftermath of the September 11th terror attacks', *European Journal of Political Economy* 20 (2): 435-446

ECB (2018) *Cyber resilience oversight expectations for financial market infrastructures*, European Central Bank, December

ESAs (2019) '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, European Supervisory Authorities, 10 April, available at https://eba.europa.eu/documents/10180/2551996/JC+2019+25+%28Joint+ESAs+Advice+on+a+coherent+cyber+resilience+testing+framework%29.pdf

EPRS (2019) 'ENISA and a new cybersecurity act', *Briefing*, 26 February, European Parliamentary Research Service

Fama, F. and K.R. French, (1992) 'The Cross-Section of Expected Stock Returns', *The Journal of Finance* 47(2): 427-465

Ferguson, R.W. (2003) '11 September, the federal reserve, and the financial system', speech on 5 February, available at: https://www.bis.org/review/r030207d.pdf

Fiott D. and R. Parkes (2019) 'Protecting Europe: the EU's response to hybrid threats', *Chaillot Paper 151,* April, European Union Institute for Security Studies

Frey B., S. Luechinger and A. Stutzer (2007) 'Calculating tragedy: Assessing the costs of terrorism', *Journal*

23 See IMF (2001), Johnston and Nedelescu (2006), Maillet and Michel (2005) and Chen and Siems (2003).

of Economic Surveys 21 (1): 1-24

Gordon L.A., M.P. Loeb, M.P.W. Lucyshyn and L. Zhou (2015) 'Externalities and the magnitude of cybers security underinvestment by private sector firms: a modification of the Gordon-Loeb model', *Journal of Information Security* 6: 24-30

He, W. (2012) 'A review of social media security risks and mitigation techniques', *Journal of Systems and Information Technology* 14(2): 171-180

Hiscox (2019) *Hiscox Cyber Readiness Report 2019,* available at https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf

IMF (2001) *World economic outlook – the global economy after 1 September: a survey by the staff of the International Monetary Fund,* World Economic and Financial Surveys 2001

Johnston R. and O. Nedelescu (2006) 'The impact of terrorism on financial markets', *Journal of Financial Crime* 12 (1): 7-25

Kopp E., L. Kaffenberger and C. Wilson (2017) 'Cyber Risk, Market Failures and Financial Stability', *Working Paper* No. 17/185, International Monetary Fund

Kaspersky (2018) *What it takes to be a CISO: Success and Leadership in Corporate IT Security Report*, available at https://www.kaspersky.com/blog/ciso-report/24288/

Leonard, M., J. Pisany-Ferry, E. Ribakova, J. Shapiro and G. B. Wolff, (2019) 'Redefining Europe's economic sovereignty', *Policy Contribution* 2019/09, Bruegel

Maillet B. and T. Michel (2005) 'The impact of the 9/11 events on the American and French stock markets', *Review of International Economics* 13(3): 597-611

Nikkinen J., M. Omran, P. Sahlstrom and J. Aijo (2008) 'Stock returns and volatility following the September 11 attacks: Evidence from 53 equity markets', *International Review of Financial Analysis* 17(1): 27-46

SonicWall (2019) *SonicWall Cyber Threat Report*, available at https://www.sonicwall.com/resources/white-papers/2019-sonicwall-cyber-threat-report/

Stiglitz, J.E. (2010) 'Risk and Global Architecture: Why Full financial Integration May Be Undesirable', *American Economic Review: Papers & Proceedings* 100: 388-392

Sunak, R. (2017) *Undersea cables: indispensable, insecure*, Policy Exchange

TD Ameritrade Institutional (2019), *RIA (Registered Investment Advisors) Sentiment Survey Report*

Verizon (2019) *2019 Data Breach Investigations Report*, available at https://enterprise.verizon.com/resources/reports/dbir/

Annex: The impact of a given cyber attack on companies' returns: econometric evidence

The release of information on a cyber attack on a company – an unexpected event – might have an impact on its stock price, as financial markets update their expectations. If such events bring additional unexpected costs for the company (both direct and indirect), stock prices will move downwards. Cyber attacks are expected to have a one-off direct cost for companies when they take place, due mostly to interrupted business activity and costs to restart activity, and also an indirect one-off cost because of reputational damage and subsequent reduction in expected demand and brand value.

Any new information on cyber attacks can impact a company's returns upon its release, months or even years after the attack originally took place. New cost estimates, for instance, or news on legal proceedings, such as legal expenses or fines, are also expected to impact a company's stock price when made public.

Econometric approach

We fit to a company's monthly returns the standard asset pricing models defined in the financial econometrics literature (Fama and French (1992) 3-Factor model). To estimate the impact of cyber attacks on a company's returns, we extend the models by adding a variable representing the severity of a cyber attack event.

The models in question are the standard CAPM:

A.1

$$(y_{it} - RF_t) = \alpha_i + \beta_i(Mkt_t - RF_t) + \gamma c_{it}$$

And the Fama and French 3-Factor model:

A.2

$$(y_{it} - RF_t) = \alpha_i + \beta_i(Mkt_t - RF_t) + \beta_{SMB} SMB_t + \beta_{HML} HML_t + \gamma c_{it}$$

Where:

Y_{it} is the market return of company at time , i.e., , with representing the stock price of company at time ;

RF_t is the risk-free rate at time , the monthly-equivalent of the 10-year US Treasury Bond rate;

MK_t is the market return at time , the market return of the S&P500 Index;

SMB_t is the Fama-French monthly *Small Minus Big* Factor, meant to control for the excess returns of small (low market cap) stock portfolios compared to big stock (large market cap) portfolios;

HML_t is the Fama-French monthly *High Minus Low* Factor, meant to control for the excess returns of large book-to-value stock portfolios compared to low book-to-value portfolios[24];

C_{it} is the variable of interest, representing the severity of a cyber attack event on company i at time t.

The variable of interest is the number of times a company has been mentioned in the media, in a given month, in cyber-attack news (see note to Figure 1 for definition of cyber-attack news). Our assumption here is that more substantial attacks are more likely to be commented on by more media outlets and more frequently. The number of mentions in the media also directly correlates with dissemination of information to the public and thus brings higher reputation costs. Variable is therefore a proxy for the severity of the cyber attack.

The companies in questions are all those which over the 2011-2019 period were mentioned in the media as targets of cyber attacks.

We got the following key results:

1. A press mention of a company in the context of a cyber attack is not enough for a statistically significant decrease in its returns. Only if a company is mentioned more than 15 times in a month in the context of a cyber attack do we find a negative effect on monthly returns.
2. We estimate that 100 mentions of a cyber attack event on a company in the media in a given month is associated with a decrease of 2.6 to 3.2 percentage points on the company's monthly returns.
3. We do not find any evidence that financial companies are more affected than non-financial companies, nor banks specifically.

24 For information on the rationale behind the factors, refer to Fama and French (1992). For information on the factors see Kenneth R. French at https://mba.tuck.dartmouth.edu/pages/faculty/ken.french/Data_Library/f-f_factors.html.