DIGITAL RESILIENCE AND FINANCIAL STABILITY. THE QUEST FOR POLICY TOOLS IN THE FINANCIAL SECTOR

José Ramón Martínez Resano

BANCO DE ESPAÑA

The author belongs to the Financial Stability and Macroprudential Policy Department. Email for comments: martinez(at)bde(dot)es.

DIGITAL RESILIENCE AND FINANCIAL STABILITY. THE QUEST FOR POLICY TOOLS IN THE FINANCIAL SECTOR

Abstract

As a result of the sweeping transition to a digitalised financial system, digital resilience is a fundamental pillar of financial stability. Achieving digital resilience poses a broad range of regulatory challenges, to respond to the complex combination of risks, essentially consisting of cyber (in)security and the concentration of computer resources in the cloud. This article presents the guiding principles of the new regulatory logic needed in the microprudential and macroprudential fields, highlighting its special features and its relationship to the exceptional combination of risks at stake in the area of digital resilience. It also discusses the need for instrumental innovations, such as greater use of circuit breakers, the singular role of cooperation in cybersecurity regulation and the unique challenges raised by the regulatory perimeter of digital resilience.

Keywords: Operational resilience, cyber resilience, cyber security, cloud.

1 Introduction

Digital resilience ranks high in the set of concerns across industries worldwide. But the new breed of risks that accompany widespread digitalisation are particularly worrying in combination with others. The concerns are magnified when considering the tight connections between traditional financial risks in the financial sector and the dangers surrounding information and communication systems (ICTs) employed for provision of financial services. Cyber space, i.e. the software-based medium that drives the "intelligence" of the services provided is often singled out as particularly challenging. Some even conceive scenarios where cyber risks are the root of the next major financial crisis (Schuermann and Mee (2018)).

Dealing with cyber and ICT risks in the financial sector or, in short, risks to digital resilience, requires new tools and metrics adapted to the interaction effects arising and the singular features of some of the new risks. These tools should complement the already broad and growing range of policies mainly dealing with technology prerequisites for successful adaptation and with the microprudential objective of developing appropriate digital risk management practices within the context of broader operational resilience programmes (BCBS (2021)).[1] This paper thus examines

1 The Basel Committee on Banking Supervision (BCBS) is following a programme to develop a coherent framework to deal with risks to basic working processes. Under the umbrella of operational resilience, the programme covers traditional operational risk management, business continuity planning and testing, third-party dependency management, incident management and resilient cyber security and ICT (here captured as digital resilience).

the ongoing quest for tools and metrics to address the risks emerging at the interface between technology and financial risks from a macroprudential vantage point. The system-wide perspective suits both the broad-based interaction and correlation effects between technology and financial vulnerabilities taking place and the level of interconnectedness that prevails.

The paper highlights the comparatively singular nature of the macroprudential measures required to deal with the interaction effects between technology and financial fragilities. In turn, it argues that these peculiarities arise largely from some singular features of shocks to digital resilience. In particular, the paper argues that the deep uncertainty regarding the probability of and losses from cyber threats calls for a stronger role for circuit breakers as a tool to contain any induced impact on financial stability. Generalised circuit breakers are intended as "time-out" rules aimed at pausing the normal course of intermediaries' business in situations where cyber incidents may put financial stability at risk.

Another noteworthy macroprudential specificity in the context of cyber risks is the comparatively greater role of cooperative tools that strengthen the ability of the community as a whole to defend itself and to recover from attacks. Providing collective IT buffers and sharing of information are two examples of collaboration highlighted. Nonetheless, traditional macroprudential instruments that limit the build-up of systemic risks in the first place like systemic risk buffers are also argued to potentially play a role provided that sound metrics have been developed for the problem.

The technological interconnectedness brought about by the new computing environments employed in the provision of digitised financial services links micro- and macro-oriented policies in singular ways. The adoption of the cloud, as the computing environment of choice by intermediaries, and the critical role played by a limited set of cloud service providers (CSPs) both elevates the systemic relevance of microprudential ICT policies and endows macroprudential ones with connotations of market structure regulation. The need to ensure a system-wide functionality that exhibits fault tolerance to individual breakdowns in a concentrated market inevitably links the micro and macro concerns in a way that blurs the ordinary limits of regulation.

The paper is organised as follows. Section 2 initially sets the scene by presenting relevant definitions and a discussion of the general nature of cyber and ICT risks, as a prelude to a discussion of the interaction between financial stability and digital resilience. Section 3, frames the various sorts policy measures (framework, micro- and macro-prudential) for dealing with digital resilience in the financial sector and examines the adequacy of traditional macroprudential tools. Then, section 4 elaborates on the need for singular macroprudential tools like circuit-breakers, collective IT buffers and rules on structure. The paper concludes by emphasising some of the challenges still besetting the quest for tools and, most notably, measurement and standardisation.

2 Digital resilience: the relevance and peculiarities of cyber and ICT risks

The importance of digital resilience is a natural outcome of the advance of digitalisation (World Economic Forum (2022)) and of two of its associated challenges, cyber and ICT risks. Cyber risk refers, broadly speaking, to the absence of cyber security in the conduct of digital operations, i.e. to risks to the confidentiality, integrity and availability of information and/or information systems (the basic triad of cyber security or "CIA") due to a cyber attack. ICT risk refers to ICT-related operational disruptions that may also put the CIA triad at risk for reasons (mostly engineering ones) unrelated to attacks.

The frequency, diversity and magnitude of some cyber incidents have led to the current situation being likened to a pandemic (Accenture (2022)). Despite the difficulties in measuring the problem, the overall phenomenology is well known in terms of scope and drivers. Both public and private, financial and non-financial entities are targets for cyber attacks by both state and non-state actors. Cases of attacks to sovereigns, health institutions, critical infrastructures abound, as revealed by existing trackers (see CSIS (2022)). Cyber incidents have kept on growing across geographical areas (see Chart 1.1) and have adapted their methods based on the pursuit of exploitive, disruptive or mixed effects (see Chart 1.2, based on the taxonomy proposed by Harry and Gallagher (2022)). Breaches compromise some or all the components of the CIA triad (see Chart 2.1). The US Congress "Solarium" report has declared that "the country is at risk, not only from a catastrophic cyber attack, but from millions of daily intrusions disrupting everything from financial transactions to the (…) electoral system" (King and Gallagher (2020)). The diversity of cyber risks is also broad as regards the business models (targeted and profit driven, attacks-as-a-service, ransomware driven, destruction driven…), the nature of the threat actions involved in the attacks (malware, hacking, social…), the attack vectors (supply chain, mobile connectivity, web services…).[2] The assets compromised exhibit a relatively stable composition over time, with incidents impacting online (servers) more intensively, followed by user and networking devices.

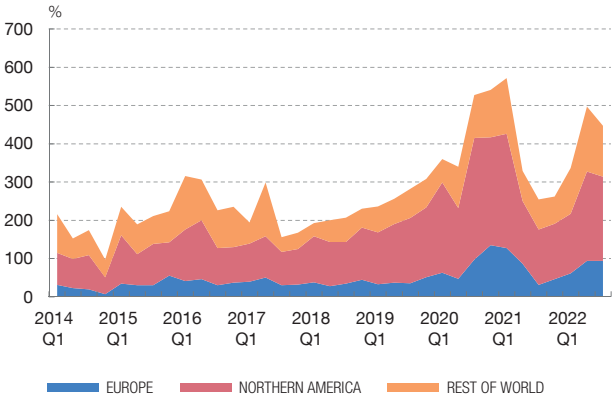
The basic distinction between cyber and ICT risks, based on the degree of intent behind their crystallization, does not imply that they are entirely independent. In addition to compromising the availability of computing resources or data, the widespread adoption of cloud computing makes this an environment that is particularly sensitive to risks, because of the concentration and interconnectedness that their scale-based business model entails.

2 The term "actions" refers to how the security incident or breach plays out. In turn, "attack vector" refers to a path that a hacker takes to exploit cybersecurity vulnerabilities. Digitalisation leads to an unavoidable expansion of the attack surface, i.e. the number of the attack vectors.

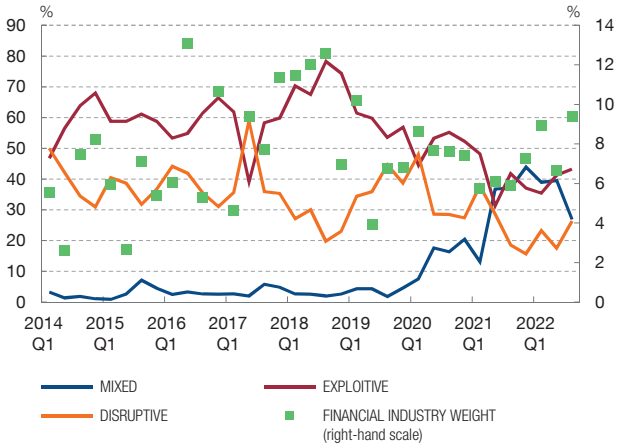
Chart 1

CYBER ATTACKS: INTENSITY AND MODALITIES

1 NUMBER OF PUBLICLY REPORTED CYBER ATTACKS ON A QUARTERLY BASIS (a)



2 DYNAMICS OF CYBER ATTACK MODALITIES ACROSS INDUSTRIES AND RELATIVE VULNERABILITY OF THE FINANCIAL SECTOR (b)



SOURCE: CISSM Cyber Events Database (University of Maryland).

a Number of breaches per quarter across geographical areas and time. See CISS (2022) and Harry and Gallagher (2022).
b Weight of exploitive, disruptive and mixed breaches in the quarterly total. See CISS (2022) and Harry and Gallagher (2022). Rhs: weight of breaches in the financial sector over the total number across sectors. A modality of attack with mixed effects can be "ransomware", the dynamics of which lately conform to those of an epidemic.

2.1 What is special about cyber shocks

The main distinctive feature of cyber shocks is the logic of intent that guides their occurrence, timing and magnitude. Their life-cycle and impact are thus crucially influenced by the original intent of the attack and its potential mutation if it is not neutralised. The traditional diffusion-based model of shock propagation, characteristic of credit and market risk models, fails to grasp the sense of purpose, intent and ingenuity that drives cyber attacks. In fact, one of the conceptual methods that is useful for quantitatively scoring the severity of cyber threats gauges the presence of such attributes (Talon (2022)).

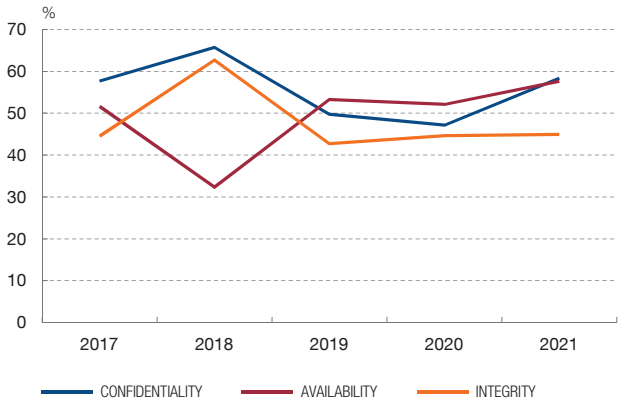
The evolution of cyber attacks may thus include special features like “smart” latency, contagion through “directed percolation”[3] and reactions to any response and/or deterrence by the victims. “Smart” latency refers to the lapse of time between system breaches and their identification, materialisation or neutralisation of economic consequences based on the attackers’ strategic calculations. Latency can achieve outstanding levels as illustrated by the endemic character attributed to some threats such as those to Log4j declared endemic despite the availability of patches (CSRB (2022)). NotPetya, one of the most damaging attacks ever recorded, is argued to have been present for several weeks in the targeted hardware. Chart 2.2 illustrates non-

3 Percolation theory describes the behaviour of clustered components in random networks.

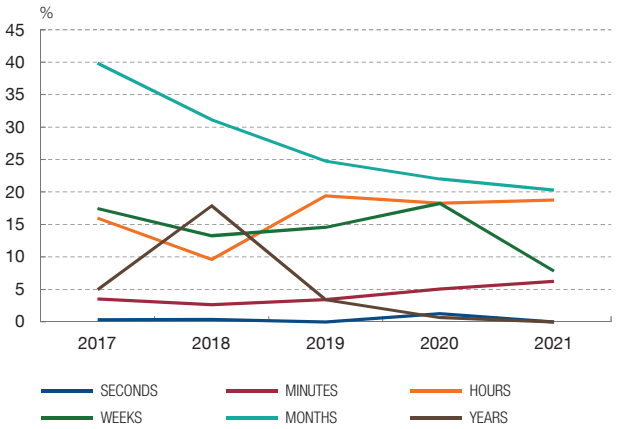
Chart 2

CYBER ATTACKS: COMPROMISED VALUES AND TIME LAG TO DISCOVERY

1 SECURITY BREACHES. BREAKDOWN BASED ON THE CIA TRIAD ACROSS TIME (a)



2 DISTRIBUTION OF TIME LAG TO BREACH DISCOVERY ACROSS YEARS (b)



SOURCE: *2022 Verizon Data Breach Investigation Report.*

a Weight of Confidentiality, Availability and Integrity breaches based on Verizon (2022).
b Percentage of breaches whose discovery takes place with various lags after occurrence. See Verizon (2022).

negligible time required to discover some breaches (Verizon (2022)). The term "percolation" describes the special process of cyber risk propagation: cyber threats are directed by attackers to transit through weak spots both within and across borders of institutions. Importantly, the percolation process exhibits an intrinsic asymmetry between defenders and attackers. The latter just need to trespass controls once to succeed in their mission. Response to and deterrence of cyber shocks shape the defensive capability to combat cyber shocks, a feature much less common in other types of shocks that also proves to be relevant to shape singularities.

The described atypical profile of cyber shocks shapes many of the challenges that explain the evolution of policies, mitigation and defence practices across sectors as well as the continuing lack of appropriate data. This evolution started with the growth of the cybersecurity industry when the first "worms" embedded in code written in the 1980s threatened early information technology users, both individual and corporate. The development of a private industry to protect IT resources has subsequently evolved in parallel to military solutions to also keep in check attacks and, in the opposite direction, to the development of a full-fledged business model for extortion and destruction even on a state-sponsored basis (Brooks (2022)). But the need to invest in private solutions to gain protection against the complexity of attacks has arguably faced the specific challenges posed by the market for security technology (Dixon (2020)). In this view, the complexity of cyber risks and cyber security would determine an information asymmetry between buyers and vendors that leads to a market breakdown (Akerlof effect) in the absence of standards and certification. Microeconomic policies that establish horizontal frameworks for the

proper functioning of security technology markets are thus instrumental for overcoming uncertainty and industry fragmentation (ECS (2021)).

Broad-based information security policies are instrumental for recognising and addressing cyber threats both as an individual and as an overall concern. In particular, they prove instrumental in overcoming the reluctance of victims to disclose information on incidents, to increase awareness and to measure the impact of breaches (Kopp, Kaffenberger and Wilson (2017)). The phenomenological characterisation of threats and impact provided by various vendors (inter alia Verizon (2022) and IBM (2022)) has helped to raise awareness although this still falls short of satisfying the need for more ambitious policy goals like those of macroprudential policies in the financial sector. Standardisation, measurement and harm quantification beyond just counting events still remain a fundamental weakness in cyber security.

The study of the transmission of cyber risks also requires new modelling approaches that could inform adapted policy approaches. Thus, the dynamics of cyber threats within a population has been found to match features of both epidemiological (Schrom et al (2021)) and securitisation market models of risk transmission (Atlantic Council (2014)). The epidemiological view of cyber risks as contagion through the exchange of code emphasises the role of collective defence and recovery whereas the securitization market analogy stresses the value of cyber design principles for security, like "zero trust" operations and transparent reporting, as a way to contain the percolation of threats. To some extent, novel policy measures against cyber risks borrow *mutatis mutandis* from similar institutions in the epidemiological and securitisation spheres. The responsibility assigned to victims in some jurisdictions to report any incident promptly to their direct partners in the supply value chain, parallels *(mutatis mutandis)* the risk retention philosophy engineered as a solution to the broad-based distribution of embedded risks characteristic of originate-to-distribute securitisation markets.

2.2 ICT and cyber risks in the financial sector

2.2.1 Digitalisation "on steroids"

Digital resilience has acquired enhanced relevance in the financial sector. The intense digitalisation of the sector together with the criticality of its services and the interconnections prevailing reinforce the concerns raised by both cyber risks and ICT outages. The accumulation of wealth managed by financial intermediaries and the general expectations that they have an unrestrained ability to offer transaction services and to preserve their vast holdings of confidential information makes of them an attractive value proposition for attackers[4] and particularly sensitive to ICT breakdowns.

4 In a nutshell, the special relevance of cyber risk for the financial sector follows the same logic as the dictum "bank robbers rob banks 'because that is where the money is'".

The frequency, diversity and magnitude of the cyber incidents in the financial sector confirms the relevance of the problem despite its moderate weight in the overall picture of attacks across sectors (see Chart 1.2). The notable efforts to quantitatively track attacks to the financial and other sectors still have to rely on publicly reported evidence based on anecdotal evidence. The Carnegie Endowment for International Peace (CEIP) compiles a tracker of publicly disclosed cyber attacks that illustrates their worldwide breadth and the moving targets (see (CEIP (2022)). The CISSM Cyber Events Database (see CISSM (2022)) attempts to lay the basis for a systematic approach to capture the effect of cyber attacks.

But expressions of concern from the industry confirm the severity of an issue where we just capture the "tip of the iceberg". The Norwegian Investment Fund puts cyber risk ahead of market risks in its list of concerns after experiencing, on average, 100,000 attacks a year, of which 1% are serious. In the field of regulators, the FCA notes a 52% increase in reports of "material" cybersecurity incidents in 2021 and expects the uptrend to continue. The public resonance of the assets compromised in some prominent cases has further raised public awareness. Significant examples of confidentiality breaches include the Target Corp. and Equifax.[5] The theft of funds in the central bank of Bangladesh epitomises the criminal high-end attack to a financial institution in an international context (Popowicz (2022)). The US also registered a massive denial of service attack and campaigns against financial messaging systems attributed respectively to Iran and North Korea.

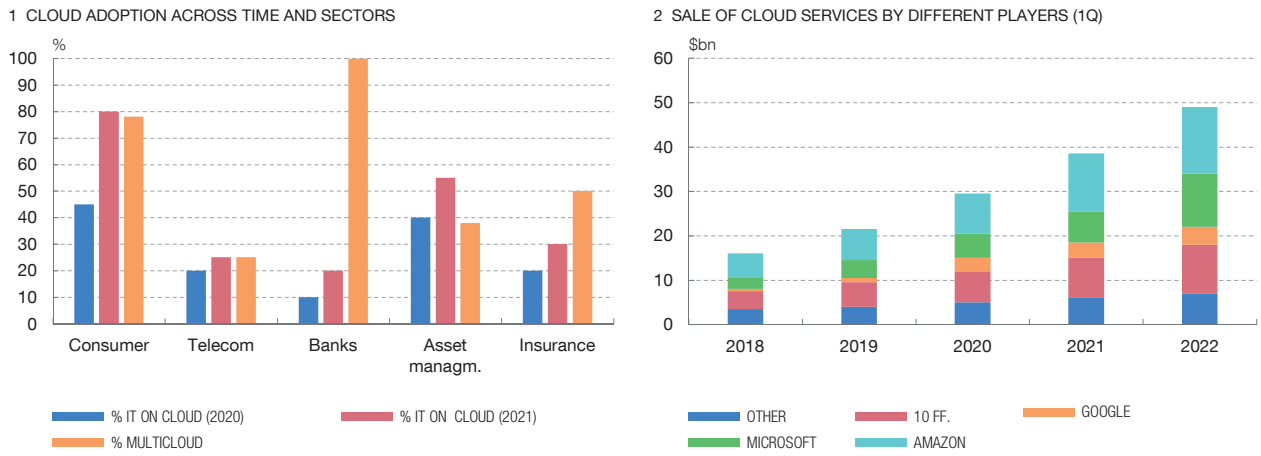
Data availability problems specifically hinder a robust estimation of financial losses due to cyber risks and impede the advancement of the cyber insurance industry. Bouveret (2018) delves into the problems while modelling aggregate losses based on a mix of actuarial and operational risk concepts. The results, based on a mix of proprietary data on losses from a consortium of banks (ORX) and on frequency of cyber attacks from a different provider, illustrates the potential for significant losses (close to 9 percent of banks' net income globally) but exclude large-scale events. However, both the methodology and the bias of the data on losses towards smaller losses (see Aldasoro et al. (2020)) limit the significance of the quantitative estimates provided, although the thrust of the analysis remains valid.

ICT-related risks have also gained prominence in the financial sector as a result of the widespread adoption of cloud computing. Cloud computing is an ICT infrastructure model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort of service provider interaction (NIST (2011)). In a nutshell, cloud computing attempts to scale up to an external context the

5 In the Target Corp case, 41 million customers' payment card accounts were breached by criminals using the credentials of 61 million Target customers that were stolen from a third-party vendor. The Equifax case sparked momentum in policy by engaging the US Senate, the CFPB and the NYDFS. 143 million US consumers had been compromised by criminals exploiting a US website application vulnerability.

Chart 3

CLOUD SERVICES: INCREASING ADOPTION AND CONCENTRATION



SOURCE: Moody's Survey and Synergy Research Group.

benefits of sharing software and servers among users, thus leading to advantages like flexibility and reduction of operating costs (CAPCO (2021)). The adoption figures in the financial sector are telling (see Chart 3.1). Data compiled by (McKinsey (2021)) show that by 2024 the average company aspires to have cloud spend represent 80 percent of its total IT-hosting budget.

Cloud computing happens to crucially condition the digital resilience of financial companies on several grounds. The concentration in the market for the provision of cloud services play a prominent role in most cases (see Chart 3.2). The market power and lock-in effects that accrue to the benefit of large third-party service providers (hyper-scalers) create an asymmetry in customers' negotiating power which could impair the ability to enforce service-level agreements that limit availability risks at reasonable costs. Choices regarding risks retained in various dimensions (service modality, control framework[6], handling of critical data[7] or handling of critical functions) can be decisive. But the basic problem of concentration through physical scaling can

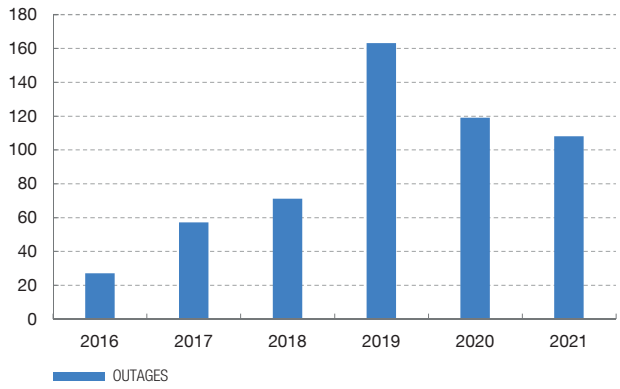
6 The service modality and the control framework refer to the involvement of customers in the exploitation of the stack (SaaS, PaaS, IaaS) and to their control rights (public, private, hybrid) over the computing facility, respectively. In SaaS (software as a service) providers' applications run on cloud infrastructure and are accessible from various client devices through web/API interfaces. The consumer neither manages nor controls the underlying cloud infrastructure including network, servers, etc. In IaaS (infrastructure as a service), there is a provision of computer processing, storage, networks, and other fundamental computing resources for the consumer to deploy and run arbitrary software, including operating systems as well as applications. The consumer neither manages nor controls the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications, and possibly some control of select networking components. PaaS (platform as a service) provides ability to deploy consumer-created applications created using programming languages, libraries, services, and tools. The consumer neither manages nor controls the underlying cloud infrastructure including network, servers, etc. operating systems, or storage but has control over the deployed applications.

7 The "location" of data influences jurisdictional powers and responsibilities arising from the CIA triad.

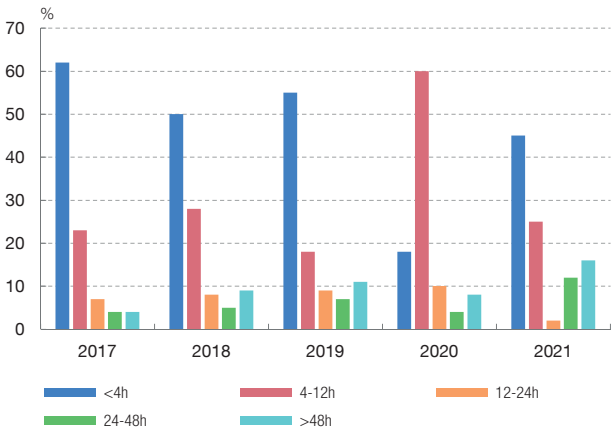
Chart 4

CLOUD OUTAGES: NUMBER AND TIME TO RECOVERY

1 NUMBER OF PUBLICLY REPORTED OUTAGES 2016-2021



2 DISTRIBUTION OF TIME TO RECOVERY FROM CLOUD OUTAGES



SOURCE: *Uptime Intelligence 2022 Outages Report.*

also crucially affect the engineering risks of the service (density of servers, power security, cooling and site construction features). Cloud adoption transfers some but not all of organizations' cyber risk since the strong security capabilities of cloud service providers must also be matched by adequate controls by providers and customers.

The advance of cloud storage and computing thus entails a comingling of ICT and cybersecurity risks with potential systemic impact. In fact, the contribution to this outcome from the mix of physical and cyber risks described in the previous paragraph has to be supplemented by that made by the complexification of the cloud market (Rogers (2022)). The recourse to multi-cloud and virtualisation techniques to mitigate the risks stemming from physical concentration and consolidate computing sites in different availability zones, leads to new risks due to an uncoordinated control of distributed computing processes. To some extent, this complexification is driven by a demand of multi-cloud multi-service choices. In a nutshell, the satisfaction of economic, functional and regulatory requirements has led to complex "cloud computing menus" that accommodate the various combinations of computing elasticity requirements and management capacity through different service modalities and control frameworks (see footnote 6).

The overall combined picture regarding digital resilience (ICT + cyber + complexification) is not entirely reassuring either in terms of clarity or risks. The increasing recourse to audits and ratings to build a picture of digital resilience in the financial sector still lacks an integrated view. But the most accurately measured component of the incidence of ICT risks (physical outages) does not provide entirely reassuring signals. Chart 4.1 drawn from a cloud services audit firm (Uptime Institute (2022)) shows the non-negligible number of publicly recorded outages, to the point that 80% of cloud customers have experienced an outage in the past three years, with about one in five

of those surveyed experiencing severe outage during the same timeframe. Significantly, the frequency and/or duration of outages might be increasing due to climate-change and energy cost reasons, inter alia (see Chart 4.2 for evidence regarding duration provided by UptimeInstitute). The lack of statistical robustness for the existing evidence does not diminish the importance of the concerns that raise the prospect of an increasingly fragile cloud industry when its use is pervasive.

2.2.2 Interplay between cyber risks and financial stability

The confluence of fragilities in digital and financial spaces heightens the significance of the former for financial sector companies. Shocks to the CIA cyber triad can trigger financial sector fragilities that largely pivot around liquidity, leverage and trust. Table 1 depicts an analytical representation of linkages between digital resilience and financial stability risks in order to guide the following discussion. Conceptually, the depicted links may operate causal effects both from the left side – i.e. technology shocks leading to the crystallisation of financial risks – and from the right, i.e. financial features inducing technological vulnerabilities. However, this paper takes the view that the former are more relevant than the latter, although section 3.2 highlights a model that stresses a role for the reverse link.

Systemic risks can unfold in this hybrid setting under a broad range of scenarios. This is essentially due to the fact that contagion effects can work now at various layers operating both in parallel and through cross-interaction. At the digital layer, digital interdependencies resulting from cyber and/or ICT connections can spread out broadly at very high speeds at the same time as they activate regular contagion channels in the financial sector. But this broader range of routes to systemic risk also exhibits a varied propensity to result in extreme effects. This diversity is largely accounted for by, for example, the lower severity of shocks to C (i.e, to data confidentiality) in comparison to shocks to I (i.e. data integrity) or to A (i.e. availability of data and systems to operate financial services). Systemic risks thus need to be qualified and not just measured.

The operation of non-linear effects further limits the chances of coming to straightforward conclusions as regards the likelihood of major events. For example, broad-based risks to data confidentiality could still damage confidence and deter the adoption of efficient financial servicing channels, causing real losses for society as a whole that exceed the outright costs of data leakages. But for this to happen, an appropriate chain of behavioural reactions among agents must take place. Although of limited use so far, agent-based models provide a general toolkit to model the endogenous reactions to attack/failure that translate various CIA shocks into liquidity and/or market value perturbations of affected intermediaries. Harmon et al. (2020) adopt this modelling framework to analyse concentration risks in the cloud. Cyber and ICT stress tests can ideally thus be grounded on micro foundations.

Table 1

INTERACTING VULNERABILITIES AND POLICIES AT THE JUNCTURE BETWEEN TECHNOLOGY AND FINANCE

The table represents two pillars of variables (technology and purely financial ones) shaping the performance and vulnerabilities of financial services. The variables in each pillar influence financial stability through their impact on vulnerabilities and amplification mechanisms of various shocks. The table intends to highlight the interaction effects between the technology and financial pillars that justify the adoption of hybrid measures, including macroprudential ones when the regular conditions of interconnection and substitutability warrant it.

	TECHNOLOGY			FINANCIAL		
	Policy	Operational	Fragility	Vulnerability	Behavioural	Policy
AMPLIFIERS	Fragmented regulation	Miopia	Complexity (supply)	Leverage	Herd behaviour	Regulatory Arbitrage
	Geopolitical confrontation	Free riding	Interconnec-tedness	Liquidity Transformation	Miopia	Market Value Accounting
	Incomplete reg. perimeter	Complexity (demand)	Attack surface	Points of Failure	Variation Margin	Regulatory Fragmentation
	Insufficient standarisation		Cloud consolidation			
DAMPENERS	Intl. Law	Cyber Governance	Encryption	Risk limits	Arbitrage	CCyRW
	Government umbrella	Cyber Ratings	Tokenisation	Capital requirements	Initial Margin	Deposit Insurance
	Regulatory Harmonisation	Cyber Frameworks	Cloud	Disclosure		Activity Restrictions
	National registers	Cooperation	IT Standards	Circuit Breakers		Liquidity Requirements
			AI	Government Support		Third Party Sector Providers

SOURCE: Own adaptation from Healey et al. (2021).

The need for agent-based models to grasp the routes to systemic instability is illustrated by the unusual outcomes taking place in shocks at the interface between the technology and financial spheres. For example, a severe cyber shock may incentivise bank creditors to run on their bank but at the same time it may disable its capacity to physically service the claims made by the customers. But such apparent neutralisation of contagion from the technology realm to the financial realm is on closer inspection only a mirage. A more granular perspective on the options available to the customers (e.g. joining the "digital queue" of bank runners, raiding other banks' operating services in anticipation of their ulterior paralysis or runs on other banks…) shows that the disruption of the supply chain caused by the cyber attack only hides the routes of contagion from the surface.

The non-linear risks associated with supply chain disruptions in the financial sector have been dealt extensively in the past in the policy space in the context of services provided by critical infrastructures. But the widespread transformation process of financial institutions adapting to the digital reality and deeper interconnections has heightened the need to deal with supply chain disruptions of regular intermediaries

consistently across the financial system. The increased interconnectivity of processes resulting from cloud computing, networking and shared software vulnerabilities brings to the forefront a distributed sense of critical arrangements in the financial system as a whole. In other words, to avoid destabilising general gridlocks in some financial functions, the reliability of individual intermediaries does not have to be absolute, but sufficient to ensure that, jointly with a quick capacity to recover from shocks, those important financial system functions do not break down. The typification of ICT processes based on their relevance for financial sector functions and the operation of intermediaries under strict reliability tolerances thus becomes a must to statistically limit knock-on effects from cyber and ICT shocks.

Widespread loss of confidence is a direct avenue linking bank fragilities and cyber-ICT shocks. The provision of liquidity services based on demand-deposit contracts is well known to be susceptible to runs driven either by panic (Diamond and Dybvig (1983)) or by fundamentals (Goldstein and Pauzner (2005)). Analysis conducted by (Duffie and Younger (2019)) and by (Koo et al. (2022)) on the ability of liquidity buffers built up under existing general regulations such as the Liquidity Coverage Ratio (LCR) and/or the current monetary policy stance to serve as a backstop has not yet sounded the alarm. But the lack of signals may be misleading due to a combination of factors, especially the ample liquidity in the banking system in the sample dates of both studies. The deposit runoff rates contained in the LCR regulations certainly provide benchmarks for assessing, based on reverse stress tests, the first-order capacity of liquidity buffers to cover outflows due to cyber shocks. More importantly, a realistic analysis of confidence shocks needs to factor in the strategic behaviour of agents.[8]

3 Policy and instruments

The importance of digital resilience warrants intense work by regulators and supervisors on both the technology and the financial side of the problem. This section provides an overview of regulatory initiatives in various dimensions. More specifically, section 3.1 briefly describes the evolving fragmentary landscape of micro-oriented rules, while section 3.2 provides the setting for macroprudential rules.

3.1 Framework and micro-oriented tools

Micro-oriented tools refer here to measures devised with individual institutions' digital “health” in mind and often arising in the context of broader operational and due diligence guidance. In turn, framework policies provide basic specifications regarding network and system operations that underpin implementations conducive to digital health. The recent accumulation of risks to digital resilience have generally

8 Eisenbach et al. (2022) make this point in the context of a shock to the operation of the Fedwire system.

led to a swift overhaul of framework rules in the US and the EU, at the same time as specific sectoral policies in the financial sector have been strengthened to deal with the relevance of digital resilience for banks. In the international context, the G7, the FSB, the Basel Committee and CPMI-IOSCO have prepared the ground by developing action principles in the quest for digital resilience[9].

Some recent landmarks of this process in Europe are the adoption of a review of rules on the security of network and information systems like NISD 2 (see EP (2022)), almost simultaneously with the agreement on the Digital Operational Resilience Act (DORA). The ECB was the front-runner in the rule-making process, with detailed guidance of cyber resilience oversight expectations for financial market infrastructures (see ECB (2018)), while the European Banking Authority has provided guidelines on ICT risk assessment (EBA (2019)), that feeds into the Supervisory Review and Evaluation process envisaged in the capital requirements Directive.[10]

The presence and mechanisms of the interaction effects between the technology and financial vulnerabilities besetting the financial sector are captured in Table 1, which represents two pillars of technology and financial variables (policies, behavioural features and vulnerabilities) that drive both the performance and vulnerabilities of financial services. The variables in each pillar influence financial stability through their impact on vulnerabilities and amplification mechanisms of various shocks. The table highlights, in particular, the potential contribution of technology policies to improve financial stability as well as the potential role of aggregate-based financial policies (inter alia macroprudential policies) aimed at feeding back in terms of a less fragile technology setup. Policy rules could thus dampen, in a hybrid fashion, the dynamics of vulnerabilities and behavioural features.

The range of relevant policy measures at horizontal level is very broad. It certainly exceeds the number of rows in Table 1 and the object of this article. Nonetheless, it helps to illustrate the plurality of rule types and even of authorities involved. Specifically, in the networks domain, the International Telecommunications Union (ITU) highlights due diligence measures and norms covering technical issues, organizational aspects, capacity-building, cooperation and legal backing that feed into comparative indexes of base country cyber resilience.[11] Unsurprisingly, such a broad landscape of cyber security frameworks and ICT rules is beset by complexity and intrinsically creates a need to provide arrangements to deal with it. Thus, the build-up of a first line of defence around technology requires certification and standardisation of solutions. Their take-up by firms requires a mix of market mechanisms and cyber hygiene regulations to build a kind of public-private partnership. In the process, the number of "framework" authorities involved increases and the coordination needs to respond

9 See G7 (2016); BCBS (2021); CPMI-IOSCO (2016).

10 See ECB (2018); EBA (2017). Calliess, C. and A. Baumgarten (2020) review the overall legislative process in Europe.

11 See ITU (2020).

swiftly to this. Computer Security Incident Response Teams (CSIRTs) and security operation centres (SOCs) are core pieces in these arrangements. Some jurisdictions have attempted to facilitate coordination with the consolidation of the multiple agencies involved within national cybersecurity centres.

Against this complex horizontal background, financial regulators and supervisors have separately strengthened their involvement in the of digital resilience policy process based on their privileged access to boards and overseers of risk management governance. The thrust of the new emerging rules applicable to cyber risks in the financial sector have thus been crafted in many respects as sector-specific rules. Nonetheless, their scope is moving beyond just due diligence considerations that target the survival of individual intermediaries to failures of entire critical functions. The new emerging regulatory notion of operational resilience encapsulates a forward-looking and functionally oriented goal to ensure fault tolerance, as opposed to the backward-looking and bag-of-risks philosophy characteristic of traditional operational risk regulations (see Peihani (2022) and Crisanto and Prenio (2017)). This new principles-based approach is facilitating the adaptation of the precise sense of rules to a complex and dynamic environment, although its commitment-based approach limits its further application from a system-wide perspective of risk. The specification of targets for key ultimate operational performance metrics (e.g. time to recovery of normal functioning) can serve the survival of individual intermediaries but be less useful from a systemic risk perspective (Prenio and Restoy (2022)).

The assurance of individual resilience has thus acquired a supervisory flavour that reflects difficulties in measuring, integrating and comparing metrics of internal performance (Venables (2022)). Against this backdrop, penetration stress testing (i.e. red team testing[12] or controlled cyber attack "simulation" like TIBER-EU) has become the most robust tool to make end-to-end security audits and supervisory assessments (Gaidosch et al. (2019)). The use of breach and attack simulation exercises has even become a commercial service for companies to remain alert on a continuous basis. Holistic rating-like tools that assess and integrate the potential for internal network risks, employee-generated risks, social engineering attacks, cloud-based attacks or third-party threats also inform the assessments.

However, cybersecurity rules aimed at individual institutions cannot avoid also pursuing the common good. Incident reporting and information sharing rules have long been deemed to be crucial to build a common defence, to the point that each EU authority concerned had its own policy (EBF (2020)). Against this backdrop, already touching upon macroprudential issues, one of the first initiatives of the European Systemic Risk Board (ESRB) in the cyber security space has been the recommendation for the establishment of a pan-European systemic cyberincident coordination framework (see ESRB (2022b)).

12 The mechanics of red team testing is described in Prenio et al. (2021).

In the EU, DORA has introduced important new orientation and harmonisation in the regulation of digital operational resilience in the EU. In particular, the sectoral contours of regulation and supervision have been pierced by the recognition and treatment of critical third-party service providers and any future guidance from supervisors on digital resilience has been strengthened with legal provisions to the effect. Thus, in addition to provisions that specify conditions formulated as *lex specialis* on cyberincident reporting and information-sharing, DORA also contains rules to strengthen the ability to deal with ICT third-party risks encountered in cloud business models. The attribution of audit rights over cloud service providers (CSPs), the strengthening of negotiating powers for service-level agreements (SLAs) with CSPs or the threat-based penetration testing of critical entities also belong to the new ample package of tools included in DORA.

3.2 Macroprudential tools

The increasing abundance of micro-focused rules for digital resilience, as outlined in section 3.1, has started to address systemic risk indirectly, through guidelines that affect critical players, like some big tech CSPs. But a robust working of the system as a whole also requires macroprudential policies addressing the externalities and interconnections arising in a fragile financial system that interacts with a brittle digital sphere.

This section elaborates on the need for tools to fight system-wide instabilities caused by the interaction of vulnerabilities on two fronts: digital and financial. The discussion on this topic in the following part of the paper must be qualified by three general observations. First, the tools considered should help prevent crisis but do not cover the deployment of crisis management tools to redress the effect of operational resilience breakdowns. Still, the preservation of incentives to manage digital resilience should remain a constraint when granting liquidity assistance in operational breakdowns, as discussed for the Bank of New York case by (Ennis and Price (2015)). Second, the nature of the macroprudential tools may vary according to the nature of shocks to digital resilience, i.e. cyber shocks and ICT shocks. Third, the suitability of regular macroprudential tools may be limited whilst new singular tools like circuit breakers, cooperative arrangements and structural measures acquire more prominence.

3.2.1 Main externalities at stake

External effects among a set of agents refers to the non-internalised and mostly indirect economic interconnections that may facilitate the propagation of shocks. They provide the basic mechanism that can lead to the transformation of more or less localised shocks into widespread systemic disruptions. The following analytical

list of external effects highlights relevant behavioural mechanisms potentially conducive to spreading of risks on the digital-financial fronts:

a) The cyber free rider problem

System-wide cyber security is a public good whose "production" depends not only on public but also on sufficiently widespread private initiatives. In fact, the maximum level of ex-ante security achievable by the community as a whole depends on the efforts made by the weakest member of the community. An imperfect substitute for the ex-ante protection granted by the recourse to cyber defence is a resilience strategy targeting just expost business continuity. But the cost undertaken to build such a strategy in terms of redundancy of resources and recovery capabilities only delivers a private good.

Anand, Duley and Gai (2022) analyse the economics of cyber contagion in a setting where a budgetary restriction on the side of intermediaries gives rise to a trade-off between the public and the private good versions of cybersecurity investment. Furthermore, they assume that the size of cyber investments by banks may also be influenced by the magnitude of their financial (rollover) risks through a relaxation-based (lower rollover risk would lower investment in cyber security) channel that might even dominate free-riding on cyber security when the liquidity risks are high.

The regulatory implications of the model are as follows. The model establishes a direct link between bank liquidity rules and investment in cyber security that creates a trade-off between the liquidity coverage ratio (LCR) and cybersecurity investment. But in the presence of heterogeneity only liquidity requirements customised to the cybersecurity profile of individual banks can be efficient. Alternatively, where free-riding prevails, regulators could achieve the efficient outcome by the imposition of appropriate duty of care penalties. Implicitly, constraining the investment in private-good resilience (pure redundancy) to a low level is also argued to lead to efficiency in the presence of closely monitored cyberhygiene guidelines or stress tests that increase incentives to invest.

b) Cyber epidemics and confidence breakdowns

Public opinion is a subtle medium as regards its role in shaping situations of systemic risk. Users of financial services can too easily experience confidence breakdowns when cyber attacks exceed thresholds of tolerance, especially if exacerbated by a state of public opinion alarm. Wolff and Demtzis (2019) depict a hypothetical but not unrealistic case of a hybrid cyber event where pure technology events and manipulation of public opinion could unleash systemic effects.

c) *Short-sighted view of risks and/or uncoordinated response to cyber shocks*

The feasibility of a continuum of cyberrisk/financial risk scenarios, ranging from scattered effects to major confidence breakdowns, broadens the spectrum of analytical and policy tools required. ESRB (2022 and 2022a) opt for testing the cyber resilience of the financial system through scenario analysis to ascertain how systemic institutions in the financial system would respond to and recover from a severe but plausible cyberincident scenario. Agent-based models can provide a methodological platform to improve these techniques based on desktop analysis.

Furthermore, the ability to undertake coordinated defence or even deterrence is a distinctive feature of cyber shocks. But a basic precondition for these strategies to succeed is the readiness to share information about the risks and attacks. However, reputational costs incurred in the process of information revelation or a lack of coordination between stakeholders can limit success in the defence of the common good. ESRB (2022) explains the vision of the EU macroprudential authority on how an incident coordination framework would facilitate an effective response to a major cyber incident.

d) *Cloud contagion*

The increasing reliance on a limited number of CSPs may bring about concentration risks for both individual intermediaries and for the financial sector as a whole. Two broad mechanisms underlying the magnification of IT risks in the cloud are correlated and cascading failures of servers. The achievement of tolerance to individual server faults has advanced based on increasing levels of redundancy and load balancing across servers (see Scott et al (2021)).

Correlation risks arise due to common factors that can eventually render redundancy useless. Segmentation of redundant servers across so-called availability zones can mitigate the risk to infrastructure features like power, cooling and network. But clouds still have an important non-infrastructure common driver: software. A oftware bug or attack can lead to correlated server failures in a distributed system. Common dependencies like DNS services are also a critical vector of attack. The isolation of workloads in individual servers may contain the direct risk of contagion and breakdown. But correlation risk through cascading failures may also create problems, i.e. computing underperformance resulting from the accumulation of backlogs of processing work across servers and delays.

Regardless of the channels through which correlation risk arises, the assessment of its likelihood and consequences in the financial sector requires active involvement of financial authorities to keep systemic risk under check (Prenio and

Restoy (2022)). The calibration of reset times after failures is a single operational resilience parameter relevant not only at the individual services provider level but also for the financial system as a whole. For example, the chaining of payments implemented through cloud micro-services can be made robust to failures capped in their duration.

3.2.2 The traditional macroprudential toolkit and cyber risks

The application of a macroprudential perspective to the regulation of digital risks in financial services provision requires adaptations to the conventional framework. The general goal of setting a system-wide safety standard with a top-down perspective in such a way that spill-overs are somehow neutralised still applies. But traditional macroprudential tools (see Krishnamurti and Lee, 2014)) do not suit the nature of the externalities at stake.

Capital buffers sensitive to cyclical patterns in the line of countercyclical capital buffers or outright exposure limits to digital risk factors cannot be operationalised to contain the external effects at play. The inertial dynamics that enables the role of cyclical buffers to curb herding behaviour does not work when the main externality at stake is free-riding. In turn, the imposition of outright limits to digital risk factors, like the ones applied under so-called borrower-based measures, can be unduly blunt and intrusive.

Arguably, a cross-sectional perspective to the design of macroprudential tools might still be useful, provided that a consistent set of indicators was available to quantify system-wide cyberrisk factors jointly with individual losses. As happens with systemic risk buffers, the logic here would be to penalise at any point of time the individual allocations of cyberrisk contamination capabilities in a manner that discourages contagion and generation of tail risks. The nature of the analysis thus relies on some mapping of internal and external cyber interconnections and dependencies. But the practical feasibility of the approach seems far-fetched at present.

4 Macroprudential tools for a singular combination of risks

This section will argue that the special profile of shocks to digital resilience warrants new approaches to macroprudential policies. In particular, this section examines the role of circuit breakers to contain contagion, the inclination to cooperate in the pursuit of system-wide stability (including through the collective provision of IT buffers) and broadening the perimeter of financial regulation beyond the financial sector.

4.1 Circuit breakers

In regulatory jargon, circuit breakers refer to provisions restricting the validity of ordinary rules during limited periods of time. Circuit breakers have found widespread application in stock market trading settings but have been much less common in banking until the introduction of resolution regimes. The main reason for this is their general association with traumatic crisis in situations where traditional shocks can unleash bank runs. This was a hindrance identified by Ize et al. (2005), who discussed whether circuit breakers in banking, i.e. temporary, efficient, and pre-programmed suspension of the convertibility of deposits could help with the management of liquidity risks of highly dollarised banking systems.

The singular nature of some large-scale cyber incidents affecting banks might also justify the interruption of the ordinary course of business in order to contain confidence breakdowns and self-fulfilling runs. The activation of a special regime linked to a large-scale cyber attack would limit in an organised, transparent and predictable way the convertibility of deposits when the event entails loss of control over the assets and the timing of recovery remains clouded by uncertainty.

Cybersecurity circuit breakers would thus complement the tepid network of regulatory, supervisory, resolution and insurance institutions that currently underpin the fragility of demand deposits. In fact, cyber-oriented circuit breakers follow a similar rationale to moratoria in recovery and resolution, i.e. the need for a pause to gather evidence on the magnitude and persistence of the damage after serious attacks.

Indeed, servicing bank deposits in non-sequential ways that limit runs is not alien to either theory or practice. Goldstein and Pauzner (2005) study the way in which general settlement rules and intermediary commitment affect the probability of runs and welfare. Under discretion over suspension of convertibility, the sequential service emerges as the optimal outcome when liquidity needs are very valuable and the liquidity of assets backing the deposits is high. The regulatory choices faced under a run, i.e. pay, stay or delay have in fact already been recognised in the context of rules on redemption gates that may ration liquidity withdrawals from money market funds under stress.

Circuit-like breakers are not entirely alien to practice or law in some jurisdictions either. Authorities can call bank moratoria in conditions unrelated to resolution proceedings and mercantile contracting frameworks worldwide also envisage clauses to deal with situations beyond the control of the parties that affect the incentives to maintain the contract unaltered. In commerce, “force majeure” clauses supersede the ordinary course of business relationships under events whose effects cannot be reasonably anticipated or controlled. A party claiming “force majeure” would need to prove that their ability to meet the contract was “impaired” or made

"impossible" due to one of the events agreed in the contract based upon the "force majeure" clause. Indeed, "force majeure" is not entirely alien to banks. For example, various trade finance model contracts issued by the International Chamber of Commerce contain such clauses adapted to and supporting the banking services at stake. Common to all these clauses is the fact that they assume that the business of the affected bank is interrupted and/or that the bank is closed for business as could happen in a large-scale cyber breach.

Admittedly, the eligibility of cyber attacks as force majeure events is not an undisputed technique to gain time after a shock. In a general commercial contracting setting one needs to exclude that the arrangement does not gives rise to moral hazard. In a cybersecurity context, the unpredictability and severity of cyber incidents might not be sufficient reason to call a pause if cyber due diligence could have avoided the damage (see Rogers and Bahar (2017)). But the capability to contain bank run contagion after large-scale cyber shocks can be sufficient justification for adding circuit breakers to the arsenal of bank regulators.

4.2 Cooperative arrangements: general incentives and shared ICT buffers

Cyber risks intrinsically entail a sort of prisoner's dilemma for targeted companies. They have both incentives to cooperate in the defence and recovery from the attack but also to follow the selfish dictates of competition. Tilting the balance between both forces typically requires the deployment of institutions by public authorities. But this endeavour faces an additional dilemma, now affecting the relationship between private and public players. Namely, the general benefits of public-private partnerships, which entail a minimum of information sharing, may also encounter reluctance among private stakeholders if they perceive that the information provided could have other non-cooperative uses (e.g. enforcement actions).

Cooperation stands out both as a significant attitude and policy orientation in the pursuit of the stability of the system as a whole in the context of cyber risks (see Rondelez (2018)). The overwhelming advance of the underlying technology threats would already justify cooperation among small to medium firms. But the alignment of incentives and the deployment of facilitating measures does not flow smoothly even in critical sectors like the financial system. Atkins and Lawson (2021) examine the faltering evolution of the public-private partnership model that deals with cyber risks in the US financial system. They document how the achievement of the current level of advance has required both the pressing force of big threats as well as a sustained and broad range of policy initiatives. But the existence of information and knowledge-sharing hubs with a broad constituency of financial sector firms, like FS ISAC, and even a selective constituency of firms dealing with systemic risk issues, like FS ARC, is a testament to the progress towards a sounder overall system.

Beyond supporting the process, Atkins and Lawson (2021) highlight the specific contribution of US regulatory policies which harmonise disparate cybersecurity standards (including on information reporting) and replace checklist-based compliance requirements with resilience judgements. A similar path may need to be covered at the international level. The dearth of standardised and complete information on threats and breaches has led to a focus on incident reporting both in Europe (ENISA (2018)) and internationally (see FSB (2021)).

An alternative based on the insurance of cyber risks by public authorities would fail to align incentives between the private and public sector. Reasons similar in nature to the ones underlying the underdevelopment of the insurance market for cyber risks would thwart the functioning of a cyber federal insurance corporation as suggested by Disparte (2017). The supporting role that public authorities have played by undertaking deterrence (see Herpig (2022)) and providing umbrella protections cannot substitute private due diligence and incentives to prevent and react to attacks.

The provision of collective ICT buffers is an example of a cooperative measure with distinct beneficial systemic effects. Collective ICT buffers can enable a significant reduction in the time needed to reboot the provision of services even after a destructive event that oversteps redundant resources built by adhering banks. A macroprudential rule that fosters the collective provision of technology buffers would compel to fund them in proportion to metrics of performance and use.

The provision of collective ICT buffers in the context of systemic risks is not an entirely new idea. In the aftermath of the global financial crisis, the systemic risks associated with the US tri-party repo system led to various reform proposals. One that finally did not come to fruition was precisely the incorporation of a shell bank (the so-called New Bank) owned by the whole industry to backstop the provision of tri-party repo services by the clearing banks.

But the provision of an extra layer of security for consumer bank accounts in the US has resulted in the provision of mutually owned infrastructure to mitigate cyberrisk effects on data availability. Sheltered Harbor is an LLC that operates under the umbrella of FS-ISAC to enhance the industry's resilience in the event of a major cybersecurity event (Nelson (2018)). In a nutshell, should a financial institution adhered to Sheltered Harbor be unable to recover from a cyber attack in timely way, it would still enable its customers to access their accounts from another member bank. The venture demonstrates in practice the strength of cooperation incentives to combat cybersecurity risks. The adoption of common data formats, secure storage of customers' data in data vaults and agreed operating processes to store and restore data overnight limits the risks from cybersecurity incidents.

4.3 Systemic technology providers and the perimeter of macroprudential policy

Macroprudential regulation cannot easily avoid overstepping its original financial sector perimeter. The framework agreed after the global financial crisis to deal with too-big-to-fail problems focused on the regulatory issues raised by both systemic banks and non-bank financial institutions (SIFIs). Emerging systemically important technological institutions (SITIs) have started to acquire increasing public policy focus as their anti-trust, sociological and/or technological externalities have gained prominence. But the interconnections between the business models and risks of financial sector intermediaries and large SITIs, like cloud "hyperscalers", implicitly broaden the institutional perimeter of macroprudential concern to SITIs.

The bonds between macroprudential oversight and technology underpinnings of financial services provision have strengthened. Prenio and Restoy (2022) envisage various alternatives to address the resulting challenges although their analysis leads them to prefer the submission of the relevant SITIs to macroprudential oversight, an approach that oversteps its traditional perimeter and that is already present in DORA and in the draft concept paper outlining supervisory powers of UK authorities in connection with third-party service providers. As a matter of fact, the alternatives also amount to a kind of intervention by financial authorities in the cloud services market. In a nutshell, and drawing on some of the service types discussed in section 2.2.1, alternative options could be to enhance the (own or external) assessments of critical providers, to promote multi-cloud services (prevailing practice nowadays) or to promote the recourse to private clouds. The winning approach will depend on new international consensus on a revamped and broader notion of the meaning of systemic and strategic that goes beyond this discussion.

The rationale to intervene in the market in the pursuit of macroprudential goals can also be demonstrated in the cybersecurity space. Kashyap and Wetherilt (2019) highlight the interest in encouraging firms to avoid common vulnerabilities and to make more diverse infrastructure (e.g. the multi-cloud argument made before) or software choices. A conceptual solution would be to penalise taking on shared risks, for example, through a concentrated use of the same software. But intervening in the market to force diversification is challenging for financial regulators. The suggested introduction of penalties in stress testing exercises based on the concentration of choices regarding software sounds more problematic than helpful.

5 Concluding remarks

Financial sector digital resilience regularly tops the rankings of systemic risk concerns. The concentration and interconnectedness of risks prompted by a shift towards cloud computing services and the pervasive intensification of cyber risks

has stimulated a broad programme of policy and regulatory measures. This paper examines the quest for tools and metrics to deal with the interaction between financial stability and technological vulnerabilities and, more specifically, it addresses the singular features of macroprudential policy for digital resilience.

The significant challenges to bolstering the individual soundness of financial intermediaries against shocks to cyber and ICT shocks through regulation have been addressed recently with intense policy impetus. In the EU, NISD 2 and DORA epitomise this trend to strengthen the basic tools and incentives of individual players to address cyber and digital operational resilience, including measures to handle the challenges posed by critical third-party service providers. Despite the proliferation of authorities involved, financial regulators and supervisors can play a crucial role in this complex regulatory process at the frontier of technology and finance thanks to their direct access to boards and their influence on financial intermediaries' risk management. But in this endeavour they still face basic measurement and standardisation problems that shape part of their regulatory agenda in the area.

The macroprudential agenda constitutes a less advanced component of the mix of concurrent tools required to ensure systemic stability. Although microprudentially oriented rules like DORA already address systemic concerns through their treatment of critical service providers, the range of externalities at stake in the cyber and ICT space raises the need for tools to address non-internalised system-wide concerns in those areas. Moreover, the singular nature of cyber and ICT risks rules out most ordinary macroprudential tools and calls for new tools or, at least, new approaches, to be considered to advance the toolkit.

Specifically, the paper examines and/or makes exploratory proposals on the potential role of circuit breakers to fight daunting large-scale cyber attacks in banking, on the opportunities raised by the distinct cooperative nature of cyber defence and on the challenges posed by the mix of cyber and ICT problems for the definition of regulatory and supervisory perimeters.

Against this backdrop, a checklist-like approach to macroprudential regulation still looks elusive. Mechanical ratios for weighting a performance metric and existing IT or financial buffers have to wait until metrics and standards are more advanced. Stress testing remains a flexible tool to accommodate both microprudential and macroprudential goals. In any event, for the macroprudential agenda, the promotion of cooperation is a productive avenue of work. The harmonisation, standardisation and enforcement of incident reporting rules should feed into the next steps for advancement. In more advanced jurisdictions, cooperation has even reached the level of building shared IT buffers.

REFERENCES

Accenture (2022). *State of Cybersecurity Report 2021.*

Aldasoro, I., L. Gambacorta, P. Giudici and T. Leach (2020). *The drivers of cyber risk,* BIS WP No. 865.

Anand, K., C. Duley and P. Gai (2022). *Cybersecurity and financial stability,* Discussion Paper 08/2022, Deutsche Bundesbank.

Atkins, S., and C. Lawson (2021). "Cooperation amidst competition: cybersecurity partnership in the US financial services sector", *Journal of Cybersecurity,* Vol. 7, No. 1

Bank of England (2022). *Operational resilience: Critical third parties to the UK financial sector,* Discussion Paper 3/2022.

BCBS (2021a). *Principles for operational resilience,* Basel Committee for Banking Supervision.

BCBS (2021b). *Revisions to the principles for the sound management of operational risk,* Basel Committee for Banking Supervision.

Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment*, Working Paper 18/143, International Monetary Fund.

Brooks, T. (2022). "The Professionalization of the Hacker Industry", *International Journal of Computer Science & Information Technology,* Vol. 14, No. 3, June.

Calliess, C., and A. Baumgarten (2020). "Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective", *German Law Journal,* Vol. 21, No. 6, pp. 1149-1179.

CAPCO (2021). *Cloud's Transformation of Financial Services.*

CEIP (2022). *Timeline of Cyber Incidents Involving Financial Institutions,* Carnegie Endowment for International Peace.

CISSM (2022). *CISSM cyber events database,* Maryland University.

CPMI-IOSCO (2016). "CPMI-IOSCO release guidance on cyber resilience for financial market infrastructures", press release.

Crisanto, J. C., and J. Prenio (2017). "Regulatory approaches to enhance banks' cyber-security frameworks", *FSI Insights,* No. 2, Financial Stability Institute.

CSIS (2022). *Significant Cyber Incidents,* Center for Strategic and International Studies.

CSRB (2022). *Review of the December 2021 Log4j Event,* Cyber Safety Review Board.

Diamond, D. W., and P. H. Dybvig (1983). "Bank Runs, Deposit Insurance, and Liquidity", *Journal of Political Economy,* Vol. 91, No. 3, pp. 401-419.

Dietrich, M., and F. Facca (eds.) (2022). *Cloud Computing in Europe: Landscape Analysis, Adoption Challenges and Future Research and Innovation Opportunities.*

Disparte, D. (2017). "A Cyber Federal Deposit Insurance Corporation Achieving Enhanced National Security", *PRISM,* Vol. 7, No. 2, pp. 52-65.

Dixon, W. (coord.) (2020). "Cybersecurity Technology Efficacy: Is cybersecurity the new 'market for lemons'?", Debate Security Forum.

Duffie, D., and J. Younger (2019). "Cyber runs: How a cyber attack could affect U.S. financial institutions", Hutchins Centre Working Papers, Brookings.

EBA (2017). *Guidelines on ICT and security risk management.*

EBF (2020). *Cyber incident reporting - EBF position (Updated version),* June.

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

ECS (2021). *A Taxonomy for the European Cybersecurity Market: Facilitating the Market Defragmentation,* February.

Eisenbach, T. M., et al. (2022). "Cyber risk and the U.S. financial system: A pre-mortem analysis", *Journal of Financial Economics,* Vol. 145, No. 3, pp. 802-826.

ENISA (2018). *Information Sharing and Analysis Center (ISACs) - Cooperative models,* Report/Study.

Ennis, H., and D. Price (2015). *Discount Window Lending: Policy Trade-offs and the 1985 BoNY Computer Failure,* No. 15-05, Federal Reserva Bank of Richmond.

EP (2022). *The NIS2 Directive: A high common level of cybersecurity in the EU,* European Parliament.

ESRB (2020). *Systemic cyber risk,* Report by the European Systemic Risk Board, February.

ESRB (2022a). *Mitigating systemic cyber risk,* Report by the European Systemic Risk Board, January.

ESRB (2022b). "ESRB recommends establishing a systemic cyber incident coordination framework", Press release of the European Systemic Risk Board, 27 January.

FSB (2021). *Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence,* Financial Stability Board, October.

G7 (2016). *G7 Fundamental Elements of Cybersecurity for the Financial Sector,* Group of 7.

Gaidosch, T., F. Adelmann, A. Morozova and C. Wilson (2019). *Cybersecurity Risk Supervision,* Staff paper, IMF, September.

Goldstein, I., and A. Pauzner (2005). "Demand-Deposit Contracts and the Probability of Bank Runs", *The Journal of Finance,* Vol. 60, No. 3, pp. 1293-1327.

Guntram, W., and M. Demertzis (2019). *Hybrid and cybersecurity threats and the European Union's financial system,* Bruegel Policy Brief.

Harmon, R. L. (2020). *Cloud Concentration Risk: A Framework Agent Based Model For Systemic Risk Analysis,* Red Hat, June.

Harry, C. T., and N. W. Gallagher (2022). *Categorizing Cyber Effects,* mimeo, CISSM Maryland University.

Healey, J., P. Mosser, K. Rosen and A. Tache (2018). "The future of financial stability and cyber risk", *The Brookings Institution Cybersecurity Project,* pp. 1-18.

Healey, J., P. Mosser, K. Rosen and A. Wortman (2021). "The Ties That Bind: A Framework for Assessing the Linkage Between Cyber Risks and Financial Stability", *Capco Institute Journal of Financial Transformation,* Vol. 53.

Herpig, S. (2021). *Active Cyber Defense Operations. Assessment and Safeguards,* Stiftung Neue Verantwortung.

IBM (2022). *Cost of a Data Breach Report 2021.*

ITU (2020). *Global Cybersecurity Index,* International Telecommunications Union.

Ize, A., E. Levy and M. A. Kiguel (2005). *Managing Systemic Liquidity Risk in Financially Dollarized Economies,* IMF, September.

Kashyap, A. K., and A. Wetherilt (2019). *Some Principles for Regulating Cyber Risk,* AEA Papers and Proceedings, Vol. 109, pp. 482-487.

King, A., and M. Gallagher (2020). *Cyberspace Solarium Commission - Report.*

Klasa, A. (2022). "Norway's oil fund warns cyber security is top concern", *Financial Times,* 22 August.

Koo, H., R. van der Molen, A. Pollastri, R. Verhoeks and R. Vermelulen (2022). *A macroprudential perspective on cyber risk,* Occasional Studies, Vol. 20-1, De Nederlandsche Bank.

Kopp, E., L. Kaffenberger and C. Wilson (2017). *Cyber Risk, Market Failures, and Financial Stability,* SSRN Scholarly Paper, No. 3024075, Rochester, NY, Social Science Research Network.

Krishnamurti, D., and Y. C. Lee (2014). *Macroprudential Policy Framework: A Practice Guide*, The World Bank (World Bank Studies), 72 p.

Matta, R., and E. C. Perotti (2019). "Pay, Stay or Delay ? How to Settle a Run", *SSRN Electronic Journal.*

McKinsey (2021). *Cloud-migration opportunity: Business value grows, but missteps abound.*

Mukhi, R., et al. (2022). "Banking Regulators Approve Final Rule Establishing Cyber Incident Notification Requirements", Vol. 139, No. 4.

Nelson, B. (2018). "FS-ISAC Testimony", Committee on Banking, Housing, and Urban Affairs, May.

NIST (2011). *The NIST Definition of Cloud Computing,* No. 800-145.

Peihani, M. (2022). "Regulation of Cyber Risk in the Banking System: A Canadian Case Study", *Journal of Financial Regulation,* Vol. 8, Issue 2, September, pp. 139-161.

Popowicz, J. (2022). "Bangladesh Bank heist casino boss faces lawsuit in New York", Central Banking.

Power, M. (2005). "The invention of operational risk", *Review of International Political Economy,* Vol. 12, No. 4, pp. 577-599.

Prenio, J., R. Kleijmeer and J. Yong (2021). *Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions,* FSI Insights, No. 21, FSI, November.

Prenio, J., and F. Restoy (2022). *Safeguarding operational resilience: the macroprudential perspective,* FSI Briefs, No. 17, FSI, August.

Rogers, O. (2022). "Why cloud is a kludge of complexity", Uptime Institute Blog.

Rogers, C., and M. Bahar (2017). *Is a cyber-attack "Force Majeure"? Je ne crois pas!,* Eversheds Sutherland.

Rondelez, R. (2018). *Governing Cyber Security Through Networks: An Analysis of Cyber Security Coordination in Belgium.*

Schuermann, T., and P. Mee (2018). "How A Cyber Attack Could Cause the Next Financial Crisis", *Oliver Wyman Risk Journal,* Vol. 8.

Schrom, E., et al. (2021). "Challenges in cybersecurity: Lessons from biological defense systems", arxiv.org

Scott, H., J. Gulliver and H. Nadler (2021). "Cloud computing in the financial sector: A global perspective", *Regtech, Suptech and Beyond: Innovation in Financial Services,* Risk.net.

Talon, M. (2022). "Cybersecurity Scoring in Plain English: On a Scale from One to Ten", Cymulate.

Toronto Centre (2020). *Cloud Computing: Issues for Supervisors.*

Uptime Institute (2022). "Annual Outage analysis 2022 - The causes and impacts of IT and data centre outages", *Risk and Resiliency,* No. 70.

Vázquez, J., and M. Boer (2018). *Addressing regulatory fragmentation to support a cyber-resilient global financial services industry,* Institute of International Finance.

Venables, P. (2022). "10 Fundamental (but really hard) Security Metrics", Risk and Cybersecurity.

Verizon (2022). *2022 Data Breach Investigations Report.*

World Economic Forum (2022). "Digital Transformation Initiative", *Digital Transformation.*

Wolff, G., and M. Demertzis (2019). *Hybrid and cybersecurity threats and the European Union's financial system,* Bruegel.