Military Cyber Affairs

Volume 3 | Issue 2 Article 7

December 2018

Dry Rivers, Scary Strangers: Are Financial And Cyber Crises Alike?

Claudia Biancotti
Bank of Italy, claudia.biancotti@bancaditalia.it

Paolo Ciocca
Consob, cioccap@gmail.com

Recommended Citation

Biancotti, Claudia and Ciocca, Paolo (2018) "Dry Rivers, Scary Strangers: Are Financial And Cyber Crises Alike?," *Military Cyber Affairs*: Vol. 3 : Iss. 2 , Article 7.
https://doi.org/10.5038/2378-0789.3.2.1061
Available at: https://digitalcommons.usf.edu/mca/vol3/iss2/7

Dry Rivers, Scary Strangers: Are Financial And Cyber Crises Alike?[1]

Claudia Biancotti[2] and Paolo Ciocca[3]

Abstract: The internet and the financial system show crucial affinities: both are tightly interconnected global networks whose orderly functioning is a prerequisite for economic prosperity. In financial and cyber crises alike, vulnerabilities are a consequence of distorted economic incentives, contagion is fast, and the most serious risk is loss of trust. Lessons learned from financial meltdowns translate to the cybersecurity world: stability cannot be achieved until policies are in place to address all of these issues. Steps have been taken to rectify incentives, as exemplified by recent European Union legislation. Data that helps identify weak nodes are still scarce, notwithstanding recent efforts. The preservation of trust is the hardest challenge: in the financial system, a global governance framework was put in place to help maintain and rebuild confidence at critical junctions, but conflicting national interests make it difficult to establish a cyber equivalent.

[1] Please cite as: Biancotti, Claudia and Paolo Ciocca, "Dry Rivers, Scary Strangers: Are Financial and Cyber Crises Alike?," in Demchak, Chris C. and Benjamin Schechter, eds. Military Cyber Affairs: Systemic Cyber Defense 3, no. 2 (2018).

[2] Senior Economist at the Bank of Italy, the Italian central bank. The views here expressed are those of the authors and should not be attributed to the Bank of Italy.

[3] Commissioner at Consob, the Italian Securities and Exchange Commission. The views here expressed are those of the authors and should not be attributed to Consob.

Advanced economies are immersed in cyberspace. In 2016, 95 percent of businesses in OECD countries had a broadband internet connection; 77 percent had a web presence. More than half of the adult population had purchased a product or service online, compared to 36 per cent in 2010[4].

As digitalization progresses, a growing share of production and consumption activities depend on connectivity. From an economist's point of view, there are evident analogies between the internet and the global financial system: both are tightly interconnected networks that provide lifeblood to the real economy, via transfers of information and funding, respectively.

Indeed, a financial crisis and a cyber crisis look alike in three key dimensions:

(i) vulnerabilities accumulate because of excessive risk-taking on the part of some agents, which eventually translates to systemic risk on account of interdependencies;

(ii) disruption can start at a single weak point and spread to the whole system in a matter of days or even hours;

(iii) the ultimate casualty is trust: once it is lost, transactions – and the whole economy – can grind to a halt as counterparties disconnect from each other.

Policy responses can be deployed to address these problems so that crises can be prevented or at least managed effectively. In the financial system, safeguards have been established over time: examples are strict capital requirements for lenders, orderly resolution procedures for failing institutions, and collection of micro-level data aimed at identification of individual weak nodes[5]. They are not all-encompassing, but they do help reduce the risk.

Where cyberspace is concerned, this process is still in its infancy. Some results have been achieved with respect to (i) above. A small but insightful literature on the economics of cybersecurity[6] points out that *distorted economic incentives, rather than technically sophisticated attacks, are at the heart of the problem.*

Software is born vulnerable because of network externalities. For products such as operating systems and messaging platforms, the value increases with the size of the installed base; developers

[4] OECD, *OECD Digital Economy Outlook 2017*, (Paris: OECD Publishing, 2017), 161-171.
[5] European Central Bank, "The Eurosystem Household Finance and Consumption Survey: Results from the First Wave" , *Statistics Papers Series* no. 2 (April 2013): 7-8.
[6] See among others: Ross Anderson, "Why Internet Security Is Hard – An Economic Perspective", *Proceedings of the 17th Annual Computer Security Applications Conference* (December 2001). Hal Varian, "Managing Online Security Risks", *The New York Times*, June 1, 2000. Tyler Moore and Ross Anderson, "Internet Security", in *The Oxford Handbook of the Internet Economy*, ed. Martin Peitz and Joel Waldfogel (Oxford: Oxford University Press, 2011).

https://digitalcommons.usf.edu/mca/vol3/iss2/7
DOI: https://doi.org/10.5038/2378-0789.3.2.1061

forego security as they scramble to get to the market first, attract a critical mass of users, and shut competition off. The absence of developer liability for buggy software does not help.

The market for cyber defense is plagued by information asymmetries. Vendors know more than their customers: they may have an opportunity to push whatever solution maximizes their own profit, independent of how effective it is. Finally, the cost of cyber attacks in many cases is not fully internalized by the immediate victims: for example, the owner of a vulnerable IoT device that gets recruited into a botnet typically has no statutory liability (yet) for damage caused by the botnet.

Some corrective measures have already been introduced, while others are being drafted. In the European Union, the General Data Protection Regulation (GDPR) – coming into force in May 2018 – imposes steep fines to businesses that put the confidentiality of personal data at risk and mandates disclosure of breaches to both authorities and data subjects. The Directive on Security of Networks and Information Systems (NIS), also coming into force this year, introduces cyber protection requirements and incident disclosure obligations for key players in sectors such as energy, finance, and healthcare. A regulation proposal put forth by the European Commission envisages an EU-wide framework for security certification of hardware and software, fashioned after the notoriously strict CE scheme for safety, health and environmental protection.

These are necessary steps, but they are not enough; the effects of GDPR and NIS are confined to certain cases or sectors. More theoretical work is needed to define broader principles: generalized liability for damage caused to third parties may be a good idea, yet an ordinary citizen whose email account gets spoofed by phishers should probably not be forced to compensate victims.

With respect to (ii), there is still a significant knowledge gap about the location and interconnections of weak nodes. As pointed out by the G7 Finance Ministers and Central Bank Governors in 2017, "*reliable, impartial, comprehensive and widely accessible*"[7] data on the frequency and economic impact of cyber attacks are still rare. The same goes for information on network and economic connections, e.g. through digital and physical supply chains.

Evidence from the Bank of Italy's business surveys suggests that cyber risk may be concentrated among high-tech, non-ICT businesses[8], which are more exposed and interesting to attackers compared to low-tech ones, and less proficient at defense than the ICT sector. The data also suggest that mass adoption of relatively simple internet-based solutions, such as e-commerce

[7] G7 Finance Ministers and Central Bank Governors, *Bari Communiqué*, May 12-13, 2017.
[8] Claudia Biancotti, "The Price of Cyber (In)security: Evidence from the Italian Private Sector", *Bank of Italy Occasional Papers* no. 407 (November 2017).

platforms, cloud computing services or IoT devices is a stronger risk factor than the selective adoption of advanced technologies, like machine learning or industrial robotics. These indications are vital in understanding which sectors of the economy need urgent intervention, be it in terms of awareness campaigns, dedicated incentives, or regulation.

The problem *sub* (iii) is the hardest to solve. After the 2009 financial meltdown, trust was only restored after a series of large-scale, highly controversial injections of public money in the banking system, and substantial reinforcement of a global governance framework which encompasses broad-based organizations such as the Financial Stability Board, the Bank for International Settlements and the International Monetary Fund, regional institutions such as the European System of Financial Supervision, and national authorities.

In a cyber crisis, there is no immediately evident equivalent of a public-sector backstop. Perhaps more importantly, a global governance framework is very hard to build because in cyberspace a crisis is generally triggered by an intentional act of aggression; an adversary is in the picture and may serve, directly or indirectly, the interests of a nation-state.

In this sense, the right comparison might be with currency or trade wars; the problem is mostly one of political, diplomatic and military relations, especially in a world where the weight of authoritarian governments increases. This is where input from economics is not sufficient and must be complemented by scholarship in the various facets of international relations.

https://digitalcommons.usf.edu/mca/vol3/iss2/7
DOI: https://doi.org/10.5038/2378-0789.3.2.1061