2021 13th International Conference on Cyber Conflict
Going Viral
T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.)
2021 © NATO CCDCOE Publications, Tallinn

The Vulnerability of the Financial System to a Systemic Cyberattack

Bobby Vedral
Managing Partner
MacroEagle Capital
PhD candidate, Modern War Studies Department
Buckingham University, United Kingdom
bobby.vedral@macroeagle.com

Abstract: The financial industry is a prime target of cybercriminal activity, mainly due to the nature of its underlying business ('that's where the money is'[1]), the sector's global interconnectedness, and its high level of digitalization. In response, the private sector has invested vast sums into cybersecurity, and regulators have started to worry about systemic risk. The latter comes in two forms. The first is the risk of a successful cyberattack against a specific financial institution 'spilling over' into the broader financial system, hence unintentionally becoming systemic. The second is the national security concern of a systemic cyberattack launched specifically to disrupt the target's financial ecosystem and therefore the real economy. In both cases, the historic evidence is clear: neither type of event has been recorded thus far. Those who consider warnings of systemic cyberattacks to be little more than threat inflation see that as vindication. This paper takes the opposite view and argues that the probability of a systemic cyberattack is significant enough to warrant a higher degree of cross-disciplinary research and preparedness. To support its main argument, this paper proposes a conceptual framework that focuses on answering two key questions. First, are there sufficient known structural vulnerabilities in the financial ecosystem that could be exploited by a willing adversary? And second, are there plausible scenarios that could see an adversarial nation-state launch such an attack? The answer to both is positive.

Given the lack of data, this analysis is largely qualitative, based on discussions with regulators, chief risk officers, academic experts, and the author's own multi-decade experience as an active participant in the financial market.

Keywords: *finance, resilience, systemic risk, vulnerabilities*

1 This was the reply of 1930s US bank robber Willie Sutton when asked why he robbed banks. He later co-authored a book titled *Where the Money Was*. See FBI History of Famous Cases & Criminals, https://www.fbi.gov/history/famous-cases [accessed 1 March 2021].

1. INTRODUCTION

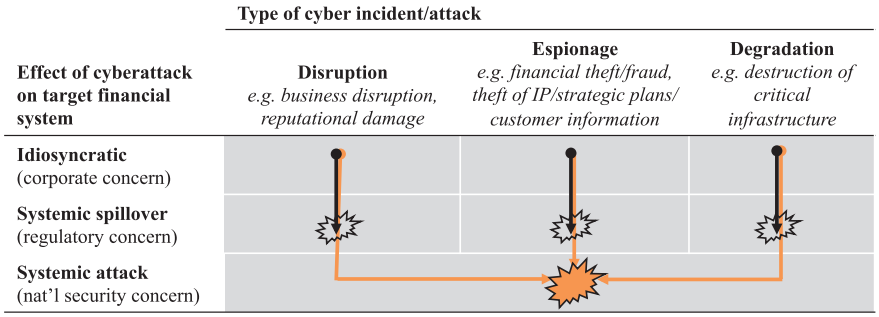
The **global financial system** lies at the heart of Western liberal democratic market economies, performing many key intermediary functions, such as deposit-taking, lending, capital markets, investments, and payments. As it is at the forefront of globalization, interconnectedness, and digitalization, its reliance on the confidentiality, integrity, and availability of data and systems is mission critical. It is therefore no surprise that national security experts have long predicted the possibility of a cyberattack on the financial system with systemic consequences, one where states would 'suffer greatly from the instability which would befall world markets should numbers be shifted in bank accounts and data wiped from international financial servers'.[2]

'Systemic cyber risk' therefore means a risk of disruption in the financial system with the potential of serious negative consequences for the real economy. This paper differentiates between two types of systemic cyber risks (see Figure 1). The first is one that starts as an idiosyncratic (company-specific) cyberattack, most probably with criminal intent but not intent to cause system-wide damage, but which inadvertently spills over to the wider financial system. This tends to be the main concern of financial regulators, given that empirical evidence points to cybercrime as the main risk. The second is the 'systemic attack', defined as a nation-state or transnational group acting with the political intent to cause severe financial instability in the target's financial markets and thus harm the real economy as well. This tends to be the main concern of the national security establishment and is the main focus of this essay. In addition, this paper defines 'cyberattack' as an event-risk/shock and not as the long-term undermining of an industry through espionage ('slow burn' or 'death by a thousand cuts').[3]

2 Jordan Schneider, as quoted in P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 191.

3 Jason Healey et al., for example, differentiate between three types of crises: slow burn (long-term undermining), exacerbated crisis (when a financial crisis is already in progress), and initiated crisis (when an adversary uses cyber capabilities to create a financial crisis). See Jason Healey, Patricia Moser, Katheryn Rosen, and Adriana Tache, 'The Future of Financial Stability and Cyber Risk', Brookings Institution, October 2018, https://www.brookings.edu/wp-content/uploads/2018/10/Healey-et-al_Financial-Stability-and-Cyber-Risk.pdf.

FIGURE 1: SYSTEMIC CRISIS BY SPILLOVER VS BY INTENT



The quantitative evidence regarding systemic cyberattacks is clear: neither a 'systemic spillover' nor a 'systemic attack' have occurred so far. But, as Figure 2 highlights, the financial sector ranks first in most studies when it comes to the frequency of cyber incidents, with most of them idiosyncratic (company specific) and criminal in nature. Also noticeable is that, probably due to the industry's high level of investment in cybersecurity, the average cost per incident is low.[4]

FIGURE 2: CROSS-SECTOR ANALYSIS OF CYBER INCIDENT FREQUENCY AND LOSSES[5]

Category	Frequency of incidents (% of total)	Total loss (% of total)	Mean loss in USD (%ile)	Standard deviation of loss in USD (%ile)
Finance & insurance	24%	16%	USD 1.69 m (10th %ile)	USD 15.45 m (13th %ile)
Most exposed sector	Finance (24%)	Professional, scientific, technical USD 8,778 m (22%)	Transportation and storage USD 16.8 m (100th %ile)	Wholesale trade USD 120.6 m (100th %ile)

This lack of systemic attacks can be attributed to three factors. First, even criminal nation-state actors, such as North Korea, need the capitalist financial system to work in order to cash out. Second, even strategic rivals, like China, need Western capitalist resources to fund their own growth; hence they have no interest in 'biting the hand that feeds them'. And third, systemic attacks on less well guarded critical national infrastructures (CNIs) may be easier to execute.

4 An excellent database for cyber incidents in the financial sector is kept by the Carnegie Endowment's 'Timeline of Cyber Incidents Involving Financial Institutions', https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline [accessed 5 January 2021].

5 For a recent global cross-sector study of cyber incidents in terms of frequencies and losses, see Iñaki Aldasoro, Leonardo Gambacorta, Paolo Giudici, and Thomas Leach, *The Drivers of Cyber Risk*, Bank of International Settlements (BIS), Working Paper No 865, May 2020, https://www.bis.org/publ/work865.htm. All loss data are in millions of US dollars (USD). Twenty sectors and 115,415 incidents are considered.

Why, then, worry about a systemic cyberattack on the financial system? To answer this question, this paper suggests a conceptual framework which defines the probability adjusted economic cost (PAEC) of such an event as a function of the expected economic cost (EEC) should it occur, times the probability of such a systemic cyberattack succeeding, i.e., the probability of a successful attack (PSA). The PSA in turn is a function of: (1) the number of structural vulnerabilities in the financial system that could be exploited; (2) the probability that an adversary has the technical ability to exploit them; (3) the probability that an adversary has the political intent to launch such an attack.

$$PAEC = EEC \times PSA\ (vulnerabilities, ability, intent)$$

Based on various conversations with financial regulators and practitioners, many agree that the key parameter in this model is 'intent'. As Tim Maurer writes, 'the main variable determining whether an actor can cause harm is not technical sophistication, not knowledge of specific vulnerabilities or development of sophisticated codes, but intent. If the intent is there, the capability will follow'.[6] Backed by the above-mentioned absence of precedent for historic systemic attacks, many practitioners point to the lack of intent as the main reason. As a chief information security officer at a major European bank wrote:

> […] the Chinese have zero interest in doing anything destructive to us or any other member of a financial system that makes them wealthy and allows them to wield political and economic influence abroad. Even Iran was circumspect in 2013 when they DDOSed US banks – the attack tech was pretty considerable, but the targets (retail banking websites) were fairly trivial. As long as GDP is a meaningful indicator to a nation-state, I don't believe that nation-state would perpetrate systemic attacks. That said, I'm sure they're curious what their rich citizens are up to, especially if that wealth could be used to aid the opposition, so it wouldn't surprise me if nation-states use espionage tactics against banks. But I can't get my head around any country just wanting to watch the system burn – even North Korea, now that they've discovered how to raise hard currency through hacking.[7]

Hence the focus of this paper is to make the case that the probability of a systemic attack is neither 'zero' nor 'very low', as the historical precedent and consensus view, respectively, imply. The argument is developed in five parts. Section 2 reviews the existing literature on systemic risk in the financial system, which broadly agrees with the assessment that the impact of such an event would be significant and that the

6 Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018), 10.

7 Chief Information Security Officer (CISO) of major Western bank, email to author, 22 December 2020.

probability is not zero. Section 3 makes the point that sufficient known vulnerabilities in the current financial ecosystem exist that could be exploited if the will to do so were there. Section 4 addresses the key question about political intent from various perspectives, including historical, cultural, and doctrinal. Section 5 concludes with some basic recommendations and suggestions for further research.

2. LITERATURE REVIEW ON 'SYSTEMIC CYBER RISK' TO THE FINANCIAL SYSTEM

Interest in 'systemic risk' took off after the Great Financial Crisis (GFC) of 2007–2008, although the focus was always more on quantifiable financial aspects, such as market, credit, and liquidity risk. Cyber risk, a sub-category of operational risk, received relatively little attention. With no commonly accepted definition of systemic risk, by **2009** the Financial Stability Board (FSB) outlined three criteria: size, substitutability, and interconnectedness.[8]

By **2013**, and following the Stuxnet disclosures, the White House issued Executive Order 13636, instructing the Department of Homeland Security (DHS) to identify those financial institutions for which a 'cyber incident would have far reaching impact on regional or national economic security'.[9] This led three years later to the creation of the Financial Systemic Analysis & Resilience Centre (FSARC), one of the first collaborative efforts in the private sector.

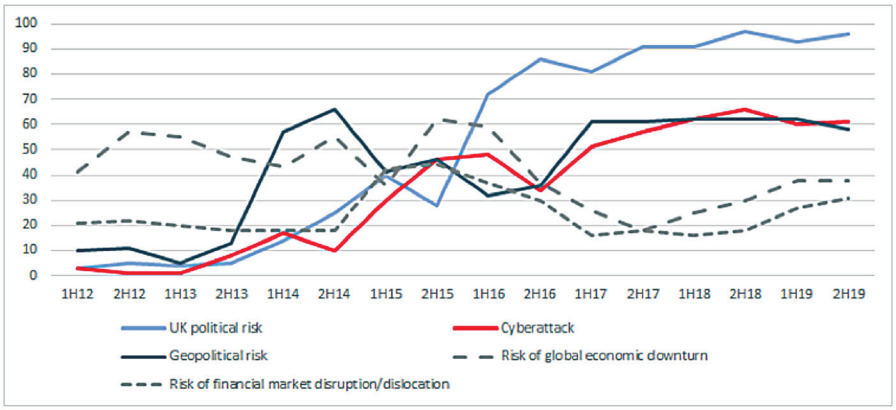
Judging by the Bank of England's (BOE) semi-annual Systemic Risk Survey (see Figure 3), 'cyberattacks' started to become prominent among financial risk practitioners in **2014**, after the cyberattack on JP Morgan. This attack, widely attributed to Iran, affected over 83 million customers.[10]

8 Financial Stability Board (FSB), 'Guidance to Assess the Systemic Importance of Financial Institutions, Markets and Instruments: Initial Considerations', IMF-BIS-FSB, October 2009, https://www.fsb.org/wp-content/uploads/r_091107d.pdf.

9 US Government, Executive Order No. 13636, 3 C.F.R. 13636 (2013), as mentioned in Jason Healey et al., 'The Future of Financial Stability and Cyber Risk'.

10 See, for example, Reuters, 'JP Morgan Hack Exposed Data of 83 Million, Among Biggest Breaches in History', 3 October 2014, https://uk.reuters.com/article/us-jpmorgan-cybersecurity/jpmorgan-hack-exposed-data-of-83-million-among-biggest-breaches-in-history-idUKKCN0HR23T20141003.

FIGURE 3: BOE SYSTEMIC RISK SURVEY – SOURCES OF RISK TO THE UK FINANCIAL SYSTEM[11]



In 2016, the year North Korea attempted to steal USD 951 million from Bangladesh's central bank,[12] the members of the G7 released the *G7's Fundamental Elements of Cybersecurity for the Financial Sector*, suggesting eight elements to follow in designing and implementing a cybersecurity program.[13] Although few academics by that time challenged the view that cyberattacks posed a systemic risk, one important exception was a 2016 *Vox* article by Danielsson et al. The article claimed that systemic cyber crises were extremely unlikely, as most cyberattacks were micro-prudential (company-specific) in nature and required extremely fortunate timing to become systemic.[14]

In 2017, the year of the WannaCry ransomware attack and Equifax hack, the International Monetary Fund (IMF) published a paper describing cyber risk as a textbook example of systemic financial stability risk and identified the main sources of vulnerabilities as access, concentration risk, correlation risk, and contagion risk.[15] Furthermore, the Institute of International Finance (IIF) published a paper that focused on the main types of scenarios that could have systemic repercussions, such as attacks

11 Bank of England (BOE), 'Systemic Risk Survey Results', 2015 H2, https://www.bankofengland.co.uk/systemic-risk-survey/2015/2015-h2; and 2019 H2, https://www.bankofengland.co.uk/systemic-risk-survey/2019/2019-h2. Note: Respondents were asked which five risks they believed would have the greatest impact on the UK financial system if they were to materialize. Answers were provided in free format and subsequently coded into the above categories by the BOE.

12 Jim Finkle, 'Cyber Security Firm: More Evidence North Korea Linked to Bangladesh Heist', Reuters, 3 April 2017, https://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea-idUSKBN1752I4 [accessed 20 December 2020].

13 G7, 'G7 Fundamental Elements of Cybersecurity for the Financial Sector', 11 October 2016, http://www.g7.utoronto.ca/finance/cyber-guidelines-2016.html [accessed 20 December 2020].

14 Jon Danielsson, Morgan Fouche, and Robert Macrae, 'Cyber Risk as Systemic Risk', *Vox*, 10 June 2016, https://voxeu.org/article/cyber-risk-systemic-risk.

15 Emanuel Kopp, Lincoln Kaffenberger, and Christoph Wilson, 'Cyber Risk, Market Failures, and Financial Stability', International Monetary Fund (IMF) Working paper No. 17/185, 7 August 2017, https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104.

on FMI, data corruption, failure of wider infrastructure, and loss of confidence.[16] Finally, the US Office of Financial Research (OFR) identified the three key financial stability risks posed by cyberattacks: lack of substitutability, loss of confidence, and loss of data integrity.[17]

By **2018** the BOE published two important papers. One warned that 'just because there has not been a clear example of a systemic impact on the sector yet, it does not mean it cannot or will not happen in the future'.[18] The second indicated a new and innovative regulatory approach in which the BOE considered the management of operational resilience to be most effectively addressed by focusing on business services rather than on systems and processes. It also announced a new regime of closer cooperation with the security services, as the lack of data required it to rely more on expert judgements.[19]

The same year also saw the publication of a widely cited Brookings paper by Jason Healey et al. identifying the three main differences between cyber and financial shocks (timing, complexity, and adversary intent) and flagging four major concerns: attacker sophistication, single points of failure, international coordination, and new technologies.[20]

Finally, that year the FSB published a 'cyber lexicon' to establish a common language and ensure consistent data collection and reliable measurement.[21] This was followed in **2019** by the International Organization of Securities Commissions (IOSCO) publishing an overview of existing frameworks for cyber regulation to serve as guidance for good practise.[22]

In **2020** the European Systemic Risk Board (ESRB) published two important and related papers, both with substantial input from the BOE. The first paper presents a conceptual model that analyses a cyber incident in four distinct phases: context,

16 Martin Boer and Jaime Vazquez, 'Cyber Security and Financial Stability: How Cyber-Attacks Could Materially Impact the Global Financial System', Institute of International Finance (IIF), September 2017, https://www.iif.com/Portals/0/Files/IIF%20Cyber%20Financial%20Stability%20Paper%20Final%2009%2007%202017.pdf?ver%3D2019-02-19-150125-767.

17 Office of Financial Research (OFR), 'Cybersecurity and Financial Stability: Risks and Resilience', OFR Viewpoint 17-01, 15 February 2017, https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf.

18 Phil Warren, Kim Kaivanto, and Dan Prince, 'Could a Cyber-Attack Cause a Systemic Impact in the Financial Sector?' Bank of England (BOE), *Quarterly Bulletin*, Q4 2018, https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2018/could-a-cyber-attack-cause-a-systemic-impact-final-web.pdf?la=en&hash=61555F2E3C15AD6B65E845C13238733B9364D4F6.

19 Bank of England (BOE), 'Building the UK Financial Sector's Operational Resilience', Discussion Paper, BOE-PRA-FCA, July 2018, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf.

20 Healey et al., 'The Future of Financial Stability and Cyber Risk'.

21 Financial Stability Board (FSB), 'Cyber Lexicon', 12 November 2018, https://www.fsb.org/2018/11/cyber-lexicon/.

22 International Organization of Securities Commissions (IOSCO), 'Cyber Task Force – Final Report', June 2019, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf.

shock, amplification, and systemic event. It then uses the model and discusses three hypothetical scenarios: (1) the incapacitation of a large domestic bank's payment system; (2) the malicious destruction of account balance data; (3) the scrambling of price and position data.[23] In the second paper, the same model is reviewed and an extensive number of systemic mitigants are listed.[24] In December, the Carnegie Endowment published a report on systemic cyber risk, identifying and providing detailed recommendations for six priority areas: cyber resilience, international norms, collective response, workforce challenges, capacity-building, and digital transformation.[25]

In summary, the existing literature shows that systemic cyber risk is a concern for financial regulators, especially those in Britain and the US, where most of the relevant publications originate from. It is also noticeable that the concern is fairly recent; most of the more in-depth studies have been produced over the last one or two years. The current paper aims to build on the existing literature in that it focuses specifically on the likelihood of a systemic attack launched by an adversarial nation-state with the intent to disrupt the target financial system. To address this question, this paper will now turn towards highlighting a number of structural vulnerabilities in the global financial system that could be exploited as either a target or an amplifier during such an attack. This goes back to this paper's conceptual model: that the probability of success is conditioned in part on the availability of vulnerabilities to exploit.

3. STRUCTURAL VULNERABILITIES IN THE FINANCIAL ECOSYSTEM

This section provides an overview of 10 known structural vulnerabilities of the financial ecosystem that highlight liberal democracies' higher exposure to financial instability due to differences in their respective political economies (openness, values), structural concentration risks (currency, geography, counterparty, participants, strategy) or amplification channels (technology, trust) across the system. The list is not meant to be exhaustive or an in-depth analysis of any one vulnerability. The intention is to highlight the fact that there is no shortage of them and that the number of possible vulnerabilities is, if anything, a parameter that increases the PSA factor in the conceptual model.

23 European Systemic Risk Board (ESRB), 'Systemic Cyber Risk', February 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

24 Greg Ros et al., 'The Making of a Cyber Crash: A Conceptual Model for Systemic Risk in the Financial Sector', European Systemic Risk Board (ESRB), Occasional Paper Series, No 16, May 2020, https://www.esrb.europa.eu/pub/pdf/occasional/esrb.op16~f80ad1d83a.en.pdf.

25 Tim Maurer and Arthur Nelson, 'International Strategy to Better Protect the Financial System against Cyber Threats', Carnegie Endowment for International Peace, 2020, https://carnegieendowment.org/files/Maurer_Nelson_FinCyber_final1.pdf.

1 – Degree of financial openness. Figure 4 compares four autocratic regimes with the main Western financial centres (US, UK) and ranks them based on military and socioeconomic criteria. Although autocratic states differ greatly in terms of economic size, they show a much tighter control over their media and financial systems, which suggests a greater degree of control in times of crisis. For example, although China has the four largest banks by assets in the world, their international expansion is minimal.[26] This contrasts with their American and European peers, who have extensive international networks. Or take North Korea, which has a record of attempting to paralyse financial networks in South Korea through cyberattacks, but whose own financial system is largely analogue and hence immune.[27]

FIGURE 4: KNOW YOUR ADVERSARY (COUNTRY'S GLOBAL RANKING BY CATEGORY)

Country	Cyber Power[28] (2020)	GDP[29] (2019)	Military Spending (2019)[30]	Press Freedom[31] (2020)	Financial Openness[32] (2018)
US	1	1	1	45	1
UK	3	6	8	35	1
China	2	2	2	177	105
Russia	4	11	4	149	85
Iran	23	29	18	173	165
North Korea	16	no data	no data	180	no data

2 – Domestic politics. Given the international exposure of Western financial institutions, it is likely that they are more vulnerable to political pressure generated by domestic conflicts, such as when consumer activism at home clashes with commercial interests overseas. For example, Beijing's 2020 imposition of a new security law in Hong Kong saw the British government lead the international condemnation, while HSBC and Standard Chartered, two British banks with significant commercial

26 Ali Zarmina, 'The World's Largest 100 Banks, 2020', S&P Global Market Intelligence, 7 April 2020, https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/the-world-s-100-largest-banks-2020-57854079.

27 As mentioned in Kong Ji Young, Lim Jong In, and Kim Kyoung Gon, 'The All-Purpose Sword: North Korea's Cyber Operations and Strategies', *11th International Conference on Cyber Conflict: Silent Battle* (Tallinn: NATO CCDCOE, 2019), 151.

28 Belfer Center, 'National Cyber Power Index 2020', Harvard Kennedy School, September 2020, https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf.

29 GDP data from 'World Development Indicators' databank, World Bank, https://databank.worldbank.org/source/world-development-indicators [accessed 30 December 2020].

30 Stockholm International Peace Research Institute (SIPRI), 'Trends in World Military Expenditure', April 2020, https://www.sipri.org/sites/default/files/2020-04/fs_2020_04_milex_0_0.pdf. Military spending measured in billions of US dollars.

31 Reporters Without Borders (RSF), '2020 World Press Freedom Index' dataset, https://rsf.org/en/ranking [accessed 20 December 2020].

32 The Chinn-Ito Financial Openness Index (KAOPEN) is an index measuring a country's degree of capital account openness and has been updated to 2018. The reference paper is Menzie D. Chinn and Hiro Ito, 'What Matters for Financial Development? Capital Controls, Institutions, and Interactions', *Journal of Development Economics* 81, no. 1 (October 2006): 163–192. The dataset is available under http://web.pdx.edu/~ito/Readme_kaopen2018.pdf.

interests in China, publicly endorsed the new law.[33] The point here is not to judge if Western institutions should have these conflicts but to highlight that they exist and to encourage further research into their implications.

3 – Currency concentration. Figure 5 provides a snapshot of the currency market, where USD 6.6 trillion is traded every day.[34] The US dollar is strongly overrepresented (when compared to US GDP), while the Chinese yuan is strongly underrepresented (when compared to China's GDP). While in the short term, this may seem to confer an advantage on the US – for instance, to be able to apply economic sanctions on countries such as Russia and Iran – there are three drawbacks. First, any loss of confidence in the US dollar would immediately have systemic repercussions. Second, the sanctions have driven Russia and China to develop their own parallel financial infrastructure, which will increase their operational independence and resilience in the future.[35] Third, a country falling under US dollar sanctions is so cut off from the global financial system that it might consider there to be no downside in attacking the system.

FIGURE 5: US DOLLAR HEGEMONY IN THE FINANCIAL SYSTEM

	% GDP (2019)[36]	Daily currency turnover, % of total (2019)	Currency as % of global reserves[37]
United States (USD)	24.4%	44.1%	60.4%
China[38] (RMB)	16.3%	2.1%	2.1%
Euro Area (EUR)	15.2%	16.1%	20.5%
All others	54.9%	37.7%	17.0%

4 – Geographic concentration. The global financial system is extremely concentrated in two markets: the US (New York), mainly for capital raising, and the UK (London), mainly for international banking, such as currency and derivative transactions. While this has clear advantages such as the clustering of expertise, it also has a major drawback

33 BBC, 'HSBC and StanChart Back China Security Laws for HK', 4 June 2020, https://www.bbc.co.uk/news/business-52916119.

34 Bank for International Settlements (BIS), 'Foreign Exchange Turnover in April 2019', Triennial Central Bank Survey, 16 September 2019, https://www.bis.org/statistics/rpfx19_fx.pdf.

35 See, for example, Russia Briefing, 'Russian and Chinese Alternatives for SWIFT Global Banking Network Coming Online', 17 June 2019, https://www.russia-briefing.com/news/russian-chinese-alternatives-swift-global-banking-network-coming-online.html/.

36 'GDP (Current USD)', as per World Development Indicators, World Bank, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?year_high_desc=true [accessed 2 July 2020].

37 'Currency Composition of Official Foreign Exchange Reserve - At a Glance - IMF Data', currency composition as per Q3 2020, IMF Currency Composition of Official Foreign Exchange Reserves (COFER) database, https://data.imf.org/?sk=E6A5F467-C14B-4AA8-9F6D-5A09EC4E62A4 [accessed 20 December 2020].

38 These numbers exclude Hong Kong SAR and the Hong Kong dollar (HKD).

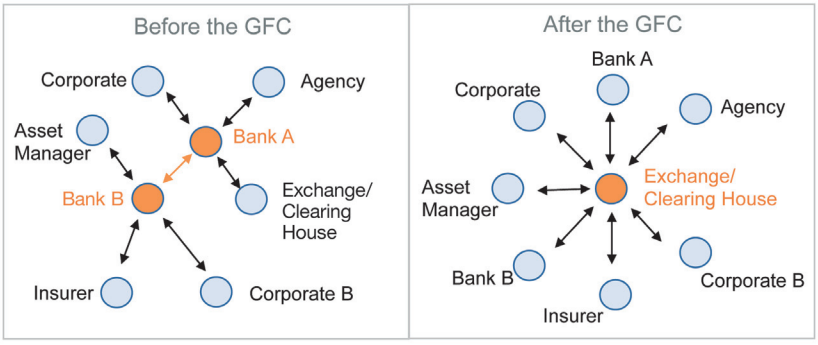
in that it offers obvious geographic targets. It is yet to be seen if the pandemic-induced trend toward remote working will endure and help reduce this vulnerability.

FIGURE 6: GEOGRAPHICAL DISTRIBUTION OF TOP FIVE FOREIGN EXCHANGE AND INTEREST RATE DERIVATIVES TURNOVER

Country	Equities[39]	FX turnover[40]	IR Derivatives[41]
United States	54.5%	26.5%	32.2%
Japan	7.7%	4.5%	1.7%
United Kingdom	5.1%	43.1%	50.2%
China (incl. Hong Kong)	4.0%	8.2%	6.0%
France	3.2%	2.0%	1.6%

5 – Central counterparty concentration. One of the key objectives of the regulatory reform efforts after the Great Financial Crisis (GFC) of 2007–2008 was to move from a trading ecosystem centred on banks and bespoke bilateral contracts to one where exchanges, central counterparties (CCPs), and standardized contracts take centre stage (see Figure 7). But while connecting firms through centralized networks makes sense, when market and liquidity risk are a regulator's key priority, it might have inadvertently created a single point of failure from an operational perspective.

FIGURE 7: SECURITIES TRADING ECOSYSTEM BEFORE AND AFTER THE GREAT FINANCIAL CRISIS (GFC)



39 Statista, 'Distribution of Countries with Largest Stock Markets Worldwide by Share of Total World Equity Market Value', January 2020, https://www.statista.com/statistics/710680/global-stock-markets-by-country/ [accessed 20 December 2020].

40 BIS, 'Foreign Exchange Turnover'.

41 Bank for International Settlements (BIS), 'OTC Interest Rate Derivatives Turnover in April 2019', Triennial Central Bank Survey, 16 September 2019, https://www.bis.org/statistics/rpfx19_ir.pdf.

6 – Market participant concentration. The financial industry is no exception to the global trend of industry concentration, usually a regulatory concern for reasons of competition and antitrust.[42] Like geographic concentration, this has the advantage of clustering expertise and ability to invest in cybersecurity. But it also means that once broken, the risk of systemic contagion is higher. Also worth considering are the network externalities of smaller financial institutions, which are probably less protected and hence more exposed. A recent Federal Reserve paper showed that under the right circumstances, a single coordinated attack on an average of 24 small institutions could lead to at least one of the top five institutions' reserves dropping below its minimum liquidity.[43]

7 – Investment strategy concentration. In the aftermath of the GFC, as banks and insurance companies de-risked, the asset management industry picked up much of the slack. At the same time, with financial conditions extremely loose (low interest rates and central bank balance sheet expansion), equity markets rose and investors shifted towards passively managed funds, increasing the amount of 'herding', as these funds merely track indices and benchmarks. A recent study by the US Federal Reserve Board noted that this active-to-passive shift meant an increased risk of amplifying market volatility (due to herding) and led to increasing industry concentration (economies of scale).[44] A cyberattack on the integrity of critical market data underlying these benchmark indices and strategies would likely paralyse much of the investment market.

8 – FinTech and Digitalization. FinTech is a relatively new term that, loosely defined, refers to technological innovations that affect financial services. These include cloud computing, robotics, artificial intelligence (AI) and machine learning (ML), mobile applications, big data analytics, blockchain or distributed ledger technology (DLT), cryptography, and quantum computing. While FinTech clearly has the potential to enhance, transform, and disrupt financial services, it also poses significant new risks. First is the risk that speed and innovation comes at the expense of safety. Second is the lack of visibility for regulators to assess technological commonalities.[45] Third is

42 See, for example, *Economist*, 'Capitalism is Becoming Less Competitive', 10 October 2018, https://www.economist.com/open-future/2018/10/10/capitalism-is-becoming-less-competitive [accessed 10 December 2020].

43 Thomas Eisenbach, Anna Kovner, and Michael Junho Lee, 'Cyber Risk and the US Financial System: A Pre-Mortem Analysis', Federal Reserve of New York, Staff Reports No 909, January 2020, https://www.newyorkfed.org/research/staff_reports/sr909.

44 Kenechukwu Andau et al., 'The Shift from Active to Passive Investing: Potential Risks to Financial Stability', Federal Reserve Board, Washington, 15 May 2020, https://www.federalreserve.gov/econres/feds/files/2018060r1pap.pdf.

45 Claudia Buch, 'Digitalization, Competition, and Financial Stability', Deutsche Bundesbank, 17 August 2019, https://www.bundesbank.de/en/press/speeches/digitalization-competition-and-financial-stability-799792.

the risk that the rapid adoption of new technology makes existing regulatory models obsolete and hence creates new risks to financial stability.[46]

9 – Automation. In July 2015 the New York Stock Exchange (NYSE) halted the trading of USD 28 trillion worth of stocks because of a coding error at Knight Capital Group, which itself declared bankruptcy a few days later. While this and various other technical flash crashes do not themselves point to anything bigger, they do reveal the fragility of the underlying reliance on high-frequency data-driven systems, quantitative algorithms, and ever-increasing trading speed, which taken together can lead to errors spreading faster and further, outpacing a management's ability to take corrective action. As Lucas Kello points out: 'A major and international interruption of stock-trading platforms could create psychological reverberations that undermine public confidence in the entire financial system.'[47]

10 – Trust. The lifeblood of financial markets is news, data, and trust. Since cyber operations allow attackers to target the integrity and/or availability of key financial data (as mentioned above) or spread misinformation, a cyberattack becomes the weapon of choice, should finance be the target. An early example of the impact of misinformation was the Syrian Electronic Army's takeover of the Associated Press's Twitter account in April 2013, sending the fake message of a bomb attack on President Obama, that caused the Dow to plunge 146 points in a few seconds, erasing USD 136 billion in market value.

As mentioned above, the point of illustrating these vulnerabilities is to flag that the financial system has various vulnerabilities that can be exploited, if the will to do so exists. In the next section, we turn to the crucial question of intent.

4. ON POLITICAL INTENT

As mentioned in the introduction, one of the most consistent pushbacks on the PSA is that most practitioners consider such an act economically irrational and hence conclude that there is little or no chance of an adversary acting this way. Six arguments can be made to argue that the probability is high enough to make the PSA and therefore the PAEC significant.

First, **historical precedent** shows the fallacy of the economic interdependence argument.[48] Henry Kissinger recently warned that the current Sino-American state of

46 Speech by Loretta J. Mester at the 2019 Financial Stability Conference in Cleveland, Ohio, 21 November 2019, https://www.clevelandfed.org/en/newsroom-and-events/speeches/sp-20191121-cybersecurity-and-financial-stability.aspx.

47 Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017), 124.

48 Exploring this argument is beyond the scope of this paper, but the roots of the interdependence argument can be found in the early 1970s. See, for example, R.O. Keohane and J.S. Nye, *Power and Interdependence* (Boston: Little, Brown, 1977).

relations bears similarities to the conditions that led to World War I.[49] Back then, well-regarded authors such as J.G. Bloch (*Is War Now Impossible?*) and Norman Angell (*The Great Illusion*) argued that economic interdependence, especially the cross-border flow of credit, technological innovation, and pure self-interest, would triumph in the face of narrow concepts of national interest and hence make war impossible.[50] It did not.

Second, nations with different histories, cultures, geographies, economies, and real or perceived threat perceptions still struggle to correctly assess other nations' **strategic interests**. Recent evidence of this includes the Iraqi invasion of Kuwait (1990), the 9/11 attacks (2001), the ISIS offensive (2014), the Russian invasion of Crimea (2014), the Chinese militarization of the South China Sea (2016), and the recent crackdown in Hong Kong (2020), most of which caught Western intelligence services by surprise. This is relevant, as some Western observers believe that China will not overreact when it comes to Taiwan. But as Coker correctly points out: 'The US palpably failed [...] in its own overreaction to 9/11. There is no "reason" to suspect the Chinese of being any more sophisticated in reasoning out what is in their best interests.'[51]

Third, a common misconception is to see a systemic attack on the financial system as an opening shot to war. However, it could just be an act of **non-violent political coercion** intended to strategically undermine another nation's will to fight by highlighting the economic cost of intervention. To return to the Taiwan example, if China wanted to send a strong message, a cyberattack would probably be preferable to a kinetic attack. As Adam Segal points out: 'In the future the moral expectation may be that states use cyber weapons before kinetic ones.'[52]

Fourth, **military doctrine** naturally evolves with technological capabilities. The 2010 military doctrine of the Russian Federation made clear that information warfare is an instrument 'to achieve political objectives without the utilization of military force'.[53] In a similar fashion, Chinese strategists speak of strategic cyber warfare being intended to 'paralyze state apparatus and [bring] about social unrest and the downfall of enemy countries' governments'.[54] According to Coker:

49 Peter Martin, 'Kissinger Warns Biden of US-China Catastrophe on Scale of WWI', Bloomberg News, 16 November 2020, https://www.bloomberg.com/news/articles/2020-11-16/kissinger-warns-biden-of-u-s-china-catastrophe-on-scale-of-wwi.

50 Lawrence Freedman, *The Future of War: A History* (Great Britain: Penguin, 2018), 42–43.

51 Christopher Coker, *The Improbable War: China, the United States and The Logic of Great Power Conflict* (London: Hurst & Company, 2015), 33.

52 Adam Segal, *The Hacked World Order* (New York: PublicAffairs, 2017), 270.

53 Segal, *The Hacked World Order*, 70.

54 Teng Jianqun and Xu Longdi, *Cyber War Preparedness, Cyberspace Arms Control and the United States* (Beijing: China Institute of International Studies, 2014), 48.

> The use of cyber-attacks is entirely consistent with Chinese strategic thinking. 'Force' ('Li') only appears nine times in Art of War's 13 chapters. As far as Sun Tzi was concerned victory and defeat are essentially psychological. The object is to inflict pain psychologically rather than physically – to put the enemy on the back foot and keep him there.[55]

Fifth, targeting the financial system allows attackers to disproportionally **target the elites**. For example, in the US, the top 10% of households owned 88.1% of stock wealth in the fourth quarter of 2019, the highest level since record-keeping began in 1989.[56] The implication of this is twofold in the case of a coercive cyberattack: either the elites will put pressure on their national government to safeguard their financial interests, or the 'bottom 90%' will put pressure to stop the financial chaos before it spreads into the real economy.

Sixth is a question of **reciprocity**. The US and UK are reported to have 'war-gamed a massive cyber strike to black out Moscow if Vladimir Putin launches a military attack on the West'.[57] One can only assume that, in the unlikely case they had not thought about it already, they have now taken notice and are planning their own measures.

5. CONCLUSION

This paper has argued that the probability of a successful systemic cyberattack (PSA) is higher than the one implied by precedent (zero) or the very low estimate given by various financial practitioners. Given that the economic impact of such an attack (EEC) would most likely be significant, any non-zero PSA implies a high enough probability adjusted economic cost (PAEC) to warrant investment into further research and preparedness planning. In fact, it is possible that the numerous observed cyberattacks on the financial sector are serving as an ongoing laboratory where malicious payloads and exploits are developed and refined in order to be used later for systemic cyberattack purposes.

Future research could consider a number of other questions. For instance, it could attempt to quantify the parameters identified in the conceptual model, where, for example, the EEC should vary from country to country given differences in the underlying economic size and structure. Moreover, an in-depth analysis could be made into any of the mentioned vulnerabilities, not only in terms of their stand-alone

55 Coker, *The Improbable War*, 160.

56 Federal Reserve, 'DFA: Distribution Financial Accounts' database, https://www.federalreserve.gov/releases/z1/dataviz/dfa/distribute/chart/ [accessed 20 December 2020].

57 Caroline Wheeler, Tim Shipman, and Mark Hookham, 'UK War-Games Cyber Attack on Moscow', *Sunday Times*, 7 October 2018, https://www.thetimes.co.uk/article/uk-war-games-cyber-attack-on-moscow-dgxz8ppv0.

impact but also considering the potential multiplier effect if two or more were targeted at the same time.

As for basic policy recommendations, three stand out. First, from the publicly available literature review, it is clear that **US and UK financial regulators** are at the forefront in terms of quantitative and qualitative analysis. That makes intuitive sense, since both host the world's major financial centres but also benefit from world-leading cybersecurity and intelligence services. NATO members' financial regulators should actively seek their advice and look for possibilities for cooperation.

Second, the ultimate backup plan against a systemic cyberattack is **to switch off** the digitalized part of the financial system while keeping the real economy running. One European financial regulator feared that the financial industry was too digitalized for this alternative to be an option.[58] But on the other hand, as recently as February 2018, Sweden's central bank governor called for public control over the country's (largely private) payment system, fearing that a fully digital system would be vulnerable to attack. He said: 'It should be obvious that Sweden's preparedness would be weakened if, in a serious crisis or war, we had not decided in advance how households and companies would pay for fuel, supplies and other necessities.'[59] Regulators should therefore consider public backup institutions on zero-trust architecture that, in an act of ultimate resilience, would allow for commercial banking to 'go manual'. A possible analogy is the response of Norsk Hydro to a March 2019 cyberattack: the Norwegian firm averted a major operational disaster by switching its plants to manual.[60] One idea would be to use the military's logistical capabilities to support the financial regulators and the private sector in providing an emergency backup banking system to the real economy during a state of emergency.

Third, cross-disciplinary scenario planning and war-gaming involving practitioners from finance, intelligence services, technology providers, and the armed forces should be encouraged. A common language should be created, and industry-specific jargon should be avoided so as not to create distance and separation in cross-disciplinary communication. Critical issues are too often misunderstood and hence remain undebated. Worst-case-scenario planning between finance, financial regulators, and national security needs to be encouraged, as economic interconnectedness and rational-choice theory are no protection against geopolitical conflict.

58 Discussion between the author and a senior European banking representative in charge of operational risk, December 2020.

59 David Crouch, 'Being Cash-Free Puts Us at Risk of Attack: Swedes Turn against Cashlessness', *Guardian*, 3 April 2018, https://www.theguardian.com/world/2018/apr/03/being-cash-free-puts-us-at-risk-of-attack-swedes-turn-against-cashlessness.

60 *Engineer*, 'Norsk Hydro Switches Plants to Manual after Cyber-Attack', 20 March 2019, https://www.theengineer.co.uk/norsk-hydro-cyber-attack/.