Military Cyber Affairs

Volume 3 | Issue 2 Article 8

2018

The Financial Sector's Vulnerabilities, Villains, and Options for Defense

John T. Harvey
Texas Christian University, j.harvey@tcu.edu

The Financial Sector's Vulnerabilities, Villains, and Options for Defense[1]

John T. Harvey[2]

Abstract: The consequences of cyber attacks on the financial sector go well beyond those suffered by the individuals and firms directly involved and may even lead to the destabilization of the system itself. The concern is all the greater given that banks and similar institutions play a much more critical role than most people realize and the nature of their operation already invites risk taking at the best of times. Bad actors hoping to sow chaos surely understand the trouble they could cause by targeting the financial underpinning of our economy. This paper will argue that while the cyber defense of the financial sector should be assigned a high priority, a wide net need not be cast since the greatest threat comes not from national actors but terrorist groups and the like. This suggests a very different strategy than one might adopt in defense of military assets or technology, an indirect approach that aims at disrupting bad actors' ability to accumulate resources, design offensive tools, and reconnoiter for possible weaknesses. Their greatest challenge is in creating sufficient time and space to plan operations with any more significance than random vandalism and DDOS attacks. Our goal should be to deny them this.

[1] Harvey, John T., "The Financial Sector's Vulnerabilities, Villains, and Options for Defense," in Demchak, Chris C. and Benjamin Schechter, eds. Military Cyber Affairs: Systemic Cyber Defense 3, no. 2 (2018).
[2] Professor of Economics, Texas Christian University

A great deal has been written about cyber security issues in the financial sector. Not only is this industry heavily dependent on the internet, but the potential rewards are very high. It is therefore not surprising to find that the bulk of cyber crime involves finance in one manner or another. Indeed, confirmed data losses in the financial industry outnumber those in the next closest competitor by more than three to one (Kopp, Kaffenberger, and Jenkinson 2017: 3). Annual costs are estimated to rise from $400 billion in 2014 to $6 trillion by 2021 (Boer and Vazquez 2017: 1).

The consequences go well beyond those suffered by the individuals and firms directly involved and may even lead to the destabilization of the financial system itself. The concern is all the greater given that banks and similar institutions play a much more critical role than most people realize. Worse yet, the nature of their operation invites risk taking at the best of times. Bad actors hoping to sow chaos surely understand the trouble they could cause by targeting the financial underpinning of our economy.

That said, the potential for retaliation and collateral damage is such that it rapidly limits the type of attackers we could reasonably expect. In general, globalization and interdependence mean that national powers would gain little by interrupting the flow of funding and commerce on which they rely as much as we do. In addition, established states like China depend heavily on the US as a market for their goods. Relations would have to deteriorate dramatically for them to be willing to take such steps (at which point the financial sector would likely be the least of our worries). Terrorist organizations and rogue states are another matter, however. They hope to create uncertainty and fear and collateral damage only adds to this. Nor do they typically use normal financial channels (Kaplan 2006). Indeed, a certain amount of discord may contribute to their ability to hide their funding sources.

This paper will therefore argue that while the cyber defense of the financial sector should be assigned a high priority, the list of suspects is limited. The greatest threat comes not from national actors but terrorist groups and similar actors. This suggests a very different strategy than one might adopt in defense of military assets or technology, an indirect approach that aims at disrupting bad actors' ability to accumulate resources, design or acquire offensive tools, and reconnoiter for possible weaknesses. Their greatest challenge is in creating sufficient time and space to plan operations with any more significance than random vandalism and DDOS attacks. Our goal should be to deny them this time and space.

https://scholarcommons.usf.edu/mca/vol3/iss2/8
DOI: https://doi.org/10.5038/2378-0789.3.2.1062

The paper proceeds as follows. First, the roles of banking and finance in the economy are outlined and the character of those sectors is discussed. Special attention is paid to inherent instabilities, which leads directly to an outline of potential vulnerabilities in the following section. Likely means of exploiting these vulnerabilities via cyber attack are then listed and possible aggressors identified. A discussion of what our most effective defense may be, and brief conclusions follow.

The Nature and Importance of the Financial Sector

John Maynard Keynes wrote that "banks hold the key position in the transition from a lower to a higher scale of activity" (Keynes 1937a: 668). Indeed they do, for production takes time and it is debt that allows the entrepreneur to build capital, hire workers, and purchase raw materials well before she has sold a single unit of output. The economy would grind to a halt if it were necessary for the prospective restauranteur to wait until she had sufficient savings to break ground. Nor are consumers anxious to wait twenty-plus years to accumulate sufficient wealth to buy a house. The builders too would prefer to sell the homes much sooner. It is the existence of a healthy financial sector that allows for the extension of credit that bridges the gap between today and tomorrow.

Surprisingly, this is a topic that is rarely addressed in mainstream economic models. For example:

> Given the prominence of debt in popular discussion of our current economic difficulties and the long tradition of invoking debt as a key factor in major economic contractions, one might have expected debt to be at the heart of most mainstream macroeconomic models—especially the analysis of monetary and fiscal policy. Perhaps somewhat surprisingly, however, *it is quite common to abstract altogether from this feature of the economy* (emphasis added; Eggertsson and Krugman 2012: 1470-1).

It is not just debt, but the role of the financial sector in general that is generally overlooked (de Araujo, O'Sullivan, and Simpson 2013; Blinder 2010, Shiller 2010, and Stiglitz 2011).[3] Since it is

[3] Although the many reasons for this lie well outside the scope of this paper, I will quickly mention two. First, the mainstream approach (also known as Neoclassicism) assumes that there is an automatic tendency for the economy to fix itself. Within this framework, they view finance as passively providing the funding necessary for the economy to move to full employment. Since it is simply acting in response to demands from the non-financial economy, they see little reason to focus on it (and instead study the latter). Second, their preferred modeling method is the general

impossible to evaluate threats to parts of the economy that are omitted from the model, this paper rejects the mainstream approach in favor of the Post Keynesian one. The latter maintains that finance, debt, and banking are indispensable parts of any explanation of the macroeconomy (see Harvey 2016 for a more extensive treatment).

As a starting point, Post Keynesians believe that it is important to make very clear the source of the funds being borrowed by businesses, households, and public-sector entities. Contrary to popular opinion, banks do not simply loan out others' savings. An understanding of the nature and importance of the financial sector is impossible without the knowledge that banks have the ability to create money from thin air, something that is both a source of flexibility and instability.

To see this, consider first the balance sheet of a typical commercial bank:

First National Bank

Assets (millions)	**Liabilities (millions)**
$60 T Bills	$200 Checking
$160 Loans	$10 Borrowed Funds
$20 Cash Reserves	$30 Net Worth
Total $240 million	Total $240 million

Assets are any items that add value to the bank while liabilities represent their obligations. *Net worth* is not a liability, per se (except in the sense that it is what the bank owes its stockholders), but shows the value of assets remaining were all liabilities to be simultaneously settled. If this number becomes negative, then the bank would be insolvent and is forced to close.[4]

equilibrium framework. This means specifying the relationships in the macroeconomy as a set of simultaneous equations. Once one has determined a solution, this becomes the point of equilibrium at which the economy could remain forever barring a parameter change. But even if we introduce the latter, this simply gives us a new equilibrium point and no explanation whatsoever regarding the process by which the adjustment occurred. More fundamentally, there was no "adjustment" at all. We simply solved two different sets of simultaneous equations. Time is irrelevant in this system and the present equilibrium does not depend in any way on past ones. Unfortunately, the very essence of the financial sector is that it links past to present to future.

[4] Note that this is not the law in every country. Even in the US a non-financial firm may remain open even though insolvent (so long as they are meeting current payment obligations). Financial institutions, however, may not.

https://scholarcommons.usf.edu/mca/vol3/iss2/8
DOI: https://doi.org/10.5038/2378-0789.3.2.1062

Assets can take a number of forms which, generally speaking, offer rates of return inverse to their relative safety. Cash (under *Reserves*) is already cash and therefore default-proof, but earns nothing. US government treasury bills (*T Bills*) are generally considered the safest asset on the planet and consequently promise a very low rate of return. *Loans* will be the bank's biggest money maker but they carry the greatest risk. Meanwhile, under liabilities banks owe their depositors whatever the latter have in their checking accounts (*Checking*) and First National Bank, too, borrows money (*Borrowed Funds*), in their case from other banks, individuals and businesses, and the Federal Reserve.

Note first that were all the bank's customers to draw on their checking accounts simultaneously, there is insufficient money in the vault to meet their demand. However, the assumption is that this is an exceedingly unlikely event, possible only during a bank run. A number of factors make the latter very rare today so that the maintenance of reserves, set by regulation at ten percent of checking deposits (http://www.federalreserve.gov/monetarypolicy/reservereq.htm), is almost an afterthought. To see why this is true, consider what happens when a bank makes a loan. Say an entrepreneur approaches the above bank with a very promising project that will require a loan of $10 million. Recalling that loans are the biggest source of income for the bank, the loan officer will want to accept this application before the entrepreneur decides to go to one of their competitors. And so she adjusts the banks balance sheet as follows (italicized numbers are changes from above):

First National Bank

Assets (millions)	**Liabilities (millions)**
$60 T Bills	*$210* Checking
$170 Loans	$10 Borrowed Funds
$20 Reserves	$30 Net Worth
Total *$250* million	Total *$250* million

Loans have risen by $10 million as has checking. The latter occurred because the manner in which the bank extended the loan was by creating–from thin air– a checking account in the amount of $10 million for the entrepreneur in question. All of this is perfectly legal for banks, who have the

power to create brand new money.[5] Indeed, it is estimated that something on the order of 97% of all our money was created by this process (see Harvey 2018 for further discussion).

The one unresolved issue is the requirement that the bank hold ten percent of deposits in reserve. However, they have fourteen days to meet this and so it does not create a realistic obstacle on the day that the loan officer acts to secure the promising loan. When they do decide to address the shortfall, the first and easiest place to look is the federal funds market, where those banks finding themselves with excess reserves will loan them overnight to those facing a shortage. Such a solution above would add $1 million to both *Reserves* (under assets) and *Borrowed Funds* (under liabilities), causing both assets and liabilities to increase to $251 million. Were the entire system to be short (as might be the case during an economic expansion), the fact that the Federal Reserve targets interest rates all but obligates them to supply the missing reserves since failing to do so would drive up rates. They would do so by purchasing Treasury bills (lowering *T Bills* by $1 million and raising *Reserves* by the same amount–total assets and liabilities would remain at $250 million).

In short, despite the emphasis placed on reserve management in many economics textbooks (and classic films!), in reality the conditions under which modern banking takes place make it almost a non-issue. Not only is a very large percentage of deposits are already guaranteed by the Federal Deposit Insurance Corporation so that depositors have no reason to rush to the teller's window, but even in the event that the system as a whole threatens to run short the central bank is obliged to supply the missing funds if they are to hit their policy target. This is very important to understand in considering potential cyber attacks. Their aim will not be something that affects reserves as that is not a point of vulnerability. *Rather, it is net worth, particularly the ratio of net worth to assets, that reflects the strength of the institution*. Recall the first balance sheet above:

[5]As do many other institutions since the repeal of Glass-Steagall–the key is the legal right to accept deposits.

https://scholarcommons.usf.edu/mca/vol3/iss2/8
DOI: https://doi.org/10.5038/2378-0789.3.2.1062

First National Bank

Assets (millions)	Liabilities (millions)
$60 T Bills	$200 Checking
$160 Loans	$10 Borrowed Funds
$20 Cash Reserves	$30 Net Worth
Total $240 million	Total $240 million

The net worth-to-asset (or capital-to-asset) ratio is $30/$240 = 12.5%. This means that First National Bank can withstand no more than a 12.5% depreciation of its assets before it becomes insolvent. And while the *Reserves* and *T Bills* are safe, the *Loans*–the bank's primary source of income–are not. Defaults and write offs could potentially push them into dangerous territory.

Here we come to the tendency toward instability. On the one hand, the ability of banks to create spending power as they do is welcome. It means that entrepreneurs and consumers do not face an artificial barrier when undertaking projects and making purchases and that the economy can therefore grow and create employment. On the other, every new loan lowers the capital-to-asset ratio. The loan officer's enthusiasm simultaneously adds money-making assets *and* balance-sheet fragility. For example, if the bank above covers the required reserves by selling T Bills, the capital to asset ratio falls from 12.5% to 12% ($30/$250); if it borrows, it becomes 11.95% ($30/$251). In either event, the transaction that places the bank in a position to earn more income also pushes them closer to insolvency. This is a key takeaway.

Even for financial institutions that do not normally take deposits (and therefore create money), the problem is the same.[6] They operate in the higher end of the market, dealing primarily with other large financial institutions and with corporations requiring advice, brokering, and other services related to funding operations. Take as an example of their operations a simplified version of Lehman Brothers position in May 2008 (they declared bankruptcy in September 2008):[7]

[6] Note that since the repeal of Glass-Steagall, there is no longer a clear legal distinction between commercial banking and other types of financial institutions. However, that does not affect the current discussion.
[7] For a more complete breakdown see pages 56 and 57 of Ball 2016.

Lehman Brothers

Assets (millions)		Liabilities (millions)	
Cash	$20,000	Short-term Borrowing	$175,000
Financial Instruments Owned	$270,000	Long-term Borrowing	$130,000
Collateralized Agreements	$300,000	Collateralized Financing	$210,000
Receivables	$40,000	Payables	$100,000
Other Assets	$14,000	Net Worth	$29,000
TOTAL	$644,000	TOTAL	$644,000

Very briefly, *Financial Instruments Owned* counts assets like securities and derivatives; *Collateralized Agreements* represents loans in exchange for temporary ownership of customer financial assets (the customer sells the asset to Lehman, then repurchases it later); *Receivables* is money owed to Lehman for various services; and *Other Assets* includes things like property. Under liabilities, *Short-* and *Long-term Borrowing* are unsecured loans (the former for under one year and the latter for over one year; roughly 80% of the *Short-term Borrowing* is Lehman taking short positions in the market, having sold an asset but not yet purchased it); *Collateralized Financing* is the reverse of *Collateralized Agreements* (it is Lehman who is selling securities on the agreement to repurchase them later); and *Payables* is money Lehman owes for various services.

Lehman's capital-to-asset ratio here is 4.5%.[8] To give an idea of just how dangerous this is, note that in a single week during the Financial Crisis the stock market lost over 20% of its value. Even in the unlikely event that this affected only *Financial Instruments Owned* and none of the other asset categories in the above portfolio, this is far more than enough to make Lehman insolvent (20% of $270 billion is $54 billion, the loss of which leave them with a net worth of -$25 billion). This highlights the dangers involved when a significant share of a financial institution's assets are traded on exchanges. While loan write offs tend to occur incrementally and presumably with some notice, the value of tradeable financial assets can change in moments.[9]

[8] In reality, various types of assets are given different weights based on their relative safety. For example, cash would receive a higher weight than treasury bills, which would receive a higher weight than stocks. Such a level of detail is not necessary here.

[9] This is also why Glass-Steagall had prohibited commercial banks from owning stocks. The goal was to ensure that

https://scholarcommons.usf.edu/mca/vol3/iss2/8
DOI: https://doi.org/10.5038/2378-0789.3.2.1062

None of this should be too worrying, of course, so long as financial institutions generate reasonably reliable forecasts of risk and return and exercise caution in building their portfolios. Unfortunately, however, there are reasons to believe that both are problematic. With respect to the first, the essential problem is that in the real world insufficient data exist to generate the objective estimates necessary to create dependable predictions. Imagine the alternative. Say, for example, that it was possible to know for sure that a particular asset had a 75% chance of appreciating by 20% and a 25% chance of appreciating by 0%. We could confidently conclude that it had an average expected rate of return of 15% ((0.75 x 20%) + (0.25 x 0%)). We may not know exactly what will happen, but we know all the possibilities and the odds of each. Assuming we knew this for a whole range of assets, we could build a portfolio that matched a target rate of return with a given appetite for risk. It would simply be a matter of plugging values into a formula. Banks and bank regulators would be able to avoid all but black-swan events.

At first glance this might seem like a reasonable approximation of the financial investment decision. Indeed, this is precisely what mainstream economic and financial models typically assume. However, Post Keynesian economists argue that this is more out of convenience than propriety and that it is one of the reasons the Financial Crisis came as such a surprise to economic orthodoxy.[10] As a well-known orthodox economist (and Nobel laureate) confessed:

> During the golden years, financial economists came to believe that markets were inherently stable — indeed, that stocks and other assets were always priced just right. There was nothing in the prevailing models suggesting the possibility of the kind of collapse that happened last year (Krugman 2009).

Those actually making the transactions were equally confident.

The real world does not allow for such mathematical certainty. We never know all the possibilities nor the odds of each, particularly when a new asset has been introduced (as with subprime derivatives). Psychology and emotion therefore play an indispensable role as we try to fill in the missing information as best we can. Without hard data to reign in decision makers, euphoria can come to dominate during successful runs and panic when there are downturns. During the former, banks and other financial institutions (and their regulators) tend to downplay the

those institutions holding the savings of the American people did not take excessive risks.

[10] Keynes, himself, makes specific reference to the "fallacies into which [one] is likely to be led" if economic decision making is assumed to be akin to calculating mathematical objective values (Keynes 1937b: 215).

possibility of negatives and view the future through rose-colored glasses. Estimates of return rise and those of risk fall. Meanwhile, when markets are pessimistic, the suddenly-negative forecasts create a rush to liquidity that can snowball into a crash. As Keynes wrote, the error of optimism "is replaced by a contrary 'error of pessimism'" (Keynes 1936: 321).

Not only are forecasts of risk and return inevitably impacted by psychological and emotional factors, thereby creating a tendency toward overreaction, but the willingness to accept the risk changes in a predictable but unwelcome manner. The Post Keynesian economist Hyman Minsky argued that as agents find that their investments are successful, so they tend to lower their risk aversion on the assumption that they had been too conservative (Minksy 1982). They may, for example, become willing to accept a higher debt-to-income ratio. Indeed, some actors may actually take on so much debt that they enter into what Minksy called the Ponzi range, where they find it necessary to continue to borrow ever increasing amounts just to service current debt repayment schedules (in anticipation of asset-price inflation sufficient to offset the cost of financing their purchase). Hence, calm periods in markets tend to cause a reduction in agents' caution.

In sum, what this means is that over periods of relative prosperity, market participants will tend to inflate predictions of return, downgrade risks, and become less risk averse. Hence, not only could we expect to see capital-to-asset ratios decline, but the optimistic forecasts driving the asset purchases will become increasingly likely to disappoint. As Minsky said, stability creates instability. If the consequences of systemic instability are sufficiently serious and widespread, this directly affects financial institutions' ability to provide funding to entrepreneurs and consumers, thus creating a general economic crisis.

Financial Sector Vulnerabilities

This is not to say that the financial sector is in a constant in a state of chaos. Keynes argued that many offsetting, stabilizing forces may exert themselves (Keynes 1936: 162-3). That said, the financial sector–a key determinant of economic growth and prosperity–ultimately consists of an interconnect series of promises where the reliability of each is evaluated on necessarily incomplete information that is colored by emotional and psychological factors. It already tends toward instability. Anyone wanting to cause mischief will not have a difficult time doing so. This paper

https://scholarcommons.usf.edu/mca/vol3/iss2/8
DOI: https://doi.org/10.5038/2378-0789.3.2.1062

focuses on four possible areas of cyber vulnerability: asset values, settlement mechanisms, support infrastructure, and market confidence.

First, critically important is the capital-to-asset ratio. Anything, therefore, that can cause a precipitous decline in a range of asset values could threaten the solvency of multiple institutions at once (as occurred during the Financial Crisis). This would severely limit the ability of financial institutions to extend the credit enterprises need in order to create output and employment (also evident during the Financial Crisis). Because of the interconnected nature of the financial system and since different kinds of institutions often exist under the same umbrella corporate group, this can affect even relatively conservative entities like the First National Bank above.

A second avenue by which one could cause havoc would be to interfere with the settlement mechanism. This is a tempting target because it is one of the areas where the financial system is relatively centralized:

> In many financial networks, a few firms or utilities serve as hubs. Their services would be hard to replace if lost or interrupted. These hubs include central banks; custodian banks; and payment, clearing, settlement, and messaging systems. Problems at key hubs can raise stability concerns (OFR 2017: 3).

Data are critical to the efficient operation of the financial system and attempts to delete or alter records of ownership, settlement prices, positions, etc., could prove to extremely disruptive.

> Nor does one have to attack the financial sector directly to score a critical hit: Direct attacks on parts of the wider infrastructure that the financial system relies upon could also result in financial stability implications. This includes attacks on utilities such as transport, telecoms, cable companies, and technology companies, including providers of data storage or cloud computing and other services (Boer and Vazquez 2017: 6).

Like actions against settlement systems, this approach simplifies the aggressor's job by providing a single avenue by which chaos can be wrought. In addition, there is a good chance that cyber defenses there are less sophisticated than those in the financial sector proper.

Fourth and last, there is the general issue of loss of confidence in the financial system. While clearly related to the above in that they can each contribute, it deserves separate treatment because of the longer-term and more widespread damage it causes. One does not have to be directly affected to feel the effects. Regardless of the means of attack, it can result in the demoralization of borrowers, lenders, and investors. While it would be an exaggeration to say that economic activity

is a result of self-fulfilling prophecy (e.g., entrepreneurs believe that sales will be high and so they hire more workers, causing sales to be higher), it does play a role and would be an obvious target. Indeed, it may be the primary one as it takes time and effort to rebuild lost confidence.

Cyber Attack Strategies

These four areas of financial-sector vulnerability suggest four possible goals of cyber attack: systemic insolvency, settlement-system breakdown, support-infrastructure failure, and catastrophic loss of confidence. How might bad actors achieve these? Note first that the issue at hand is not cyber crime. While theft certainly does not contribute to financial stability and although widely publicized incidents of dramatic, large-scale losses of data or funds can prove damaging, the presumed goal of those perpetrators is not to damage the US economy but to enrich themselves. The concern here is with forces whose goals are destruction and destabilization.

Table I in Valeriano and Maness 2014 (recreated below; p.353) defines five types of cyber attacks:[11]

[11] They list seven categories, but the last two are combinations of previous ones.

https://scholarcommons.usf.edu/mca/vol3/iss2/8
DOI: https://doi.org/10.5038/2378-0789.3.2.1062

Table 1. Cyber methods for incidents and disputes

Type of dispute	**Examples**	**Explanation**
1 Vandalism	Website defacements	SQL injection or cross-scripting to deface websites
2 Denial of service	DDoS, distributed denial of service	Botnets used to effectively shut down websites with high traffic
3 Intrusion	Trapdoors or Trojans, backdoors	Remotely injected software for intrusions and thefts
4 Infiltrations	Logic bombs, worms, viruses, packet sniffers, keystroke logging	Different methods are used to penetrate target networks. Can be remotely used or physically installed
5 APTs	Advanced persistent threats	Precise methods that have specific targets. Move slowly to avoid detection, can be vandalism, DDoS, intrusions, or infiltrations

As already noted, the financial sector is witness to the highest volume of attacks. Most are of the first two types listed above. In a piece entitled "DDoS is most common cyber attack on financial institutions," Warwick Ashford writes:

> Even though DDoS attacks are often associated with large organisations, research shows that 51% of all companies (no matter the size) have experienced an attack and 70% of DDoS attack victims are targeted more than once, the security firm said in a blog post (Ashford 2016).

This is therefore an area of emphasis for the IT departments at banks and financial institutions and so recovery is generally pretty fast. DDoS attacks and vandalism–unless they could be perpetrated repeatedly over a long period of time and across various institutions–are unlikely to achieve the goal of disrupting the entire financial system.[12]

This leaves intrusion, infiltrations, and APTs as the most likely avenues of assault (where the last really describes a carefully targeted campaign rather than a single specific method). There have been a number of historical incidents, albeit most with the goal of financial gain rather than

[12] A broader-based attack may well include these, of course.

financial system breakdown. However, they are instructive when thinking about how one of the above goals–systemic insolvency, settlement-system breakdown, support-infrastructure failure, and catastrophic loss of confidence–may be achieved. Perhaps the most famous example was the attack on the SWIFT (Society for Worldwide Interbank Financial Telecommunications) system in Bangladesh, which netted the thieves $81 million. This would be akin to an attack on the settlement system and represents an infiltration (and more generally an APT).[13] The malware in question, Dridex, was activated when targeted email recipients opened Word or Excel attachments. Sensitive information was then stolen and used to undertake fraudulent transactions. In addition, "hackers infected the system with malware that disabled the SWIFT printer. Bank officials in Dhaka initially assumed there was simply a printer problem" (Varadhan 2018). The stolen cash then "disappeared into the casino industry in the Philippines" (Varadhan 2018). An attack on India's City Union Bank followed a similar pattern and, as is common in such cases, it was some time before the IT department even realized that there was a problem (Varadhan 2018).

Hackers in 2014-5 used an approach by which one might be able to cause systemic insolvency. They used a Trojan (Corkow) to manipulate the dollar-ruble exchange rate via a Russian trading system terminal (ENISA 2016). The latter was infected as a result of "drive-by downloads, whereby machines get infected when victims visit compromised, and often legitimate websites" (ENISA 2016). Similar events had occurred in the US in 2010 and Russia in 2012, and were someone more interested in creating havoc than amassing a fortune then it would not be difficult to set into motion an asset deflation that threatened the stability of the financial sector. This is especially true given how many automated sell signals would be triggered once an initial round of sales had been undertaken by the attacker. One only has to start the ball rolling. Like the Bangladesh SWIFT incident, this was an infiltration (and APT) that made use of a key logger.

We also have examples of attacks on infrastructure. As recently as March 15, 2018, the Trump administration announced that the Russians had been attacking the US power grid going back a number of years and had the capability of shutting down or sabotaging some plants at will (Perlroth and Sanger 2018). Reports indicate that their tactics were "remarkably similar to those employed by Russia when it took down parts of Ukraine's electrical grid in 2015 and 2016. In the

[13] Strictly speaking, these were not attacks on the settlement system, per se, but efforts to make use of it to undertake fraudulent entries at the level of individual banks. But there is nevertheless sufficient overlap to consider it in this category.

https://scholarcommons.usf.edu/mca/vol3/iss2/8
DOI: https://doi.org/10.5038/2378-0789.3.2.1062

second attack, Russian hackers employed malicious software to carry out a fully automated assault on the power grid in Kiev" (Raphelson 2018). In the US case, there is some indication that the Russian efforts were oriented toward reconnaissance, learning how systems operate, and positioning themselves to act later. These incidents, too, like those discussed above, appear to have been in the form of an infiltration and perhaps preliminary steps in a more focused APT.

Attacks aimed at creating a loss of confidence are in many ways simply the longer-term, indirect consequence of those focusing on systemic insolvency, settlement-system breakdown, and support-infrastructure failure. That said, in cyber conflicts it is often the indirect effects that represent the primary goal (Lin 2012: 37-41). Indeed, direct effects can usually be corrected fairly quickly. Computers can be cleaned of viruses, passwords changed, and services restored in hours or days, but regaining confidence may require many incident-free months. Even then, the fact that breaches by sophisticated actors can take years to discover means that everyone is continuously looking over their shoulders.

Campaigns aimed at attacking credibility and reliability may require multiple avenues and repeated efforts over an extended period of time. Perhaps the closest example of this may be the series of cyber intrusions North Korea has (allegedly) made into South Korea. In 2013, for instance, cyber attackers (suspected to be either the North Korean government or patriotic hacktivists) took down two South Korean television broadcasters and three banks (Sang-Hun 2013). No financial gain was sought. Rather, it was likely meant to be a political statement, particularly as it coincided with US and South Korean military maneuvers. More recently, it is strongly suspected that North Korea was behind attacks on South Korean cryptocurrency exchanges (Ashford 2018). And while they have not limited their attention to the southern half of the peninsula, it is rumored that they have at least one unit–Labyrinth Chollima–that is specifically South-Korea focused (Dilanian 2018).

Though these efforts included targets other than the financial sector and some of the intrusions appeared more criminal than political, they nevertheless suggest how an attacker can spark and then nurture an atmosphere of doubt and fear. Taken as a whole, they have established North Korea–clearly an economic and military inferior to the South Korean-US alliance–as a force to be reckoned with in cyberspace (see for example Capaccio 2018, Dilanian 2018, Fifield 2018,

and Sanger, Kirkpatrick, and Perloth 2017). Indeed, a recent South Korean editorial lamented their lack of cyber security and the ease with which the North reaches into the South:

> That North Korea stole cyber currency from the South's exchanges and attempted to launder cryptocurrency it stole overseas in the South is as good as a provocation in the form of taking assets from people in the South. It is absolutely imperative that a president and his or her administration protects the life and property of the people. If they sat on their hands as the people's property was taken by North Korean hackers, it is a gross dereliction of duty. The history of the North's cyberattacks is not short (Korea Herald 2018).

This is most certainly precisely what Pyongyang hoped to achieve.

Possible Cyber Villains: Rouge States?

What North Korea accomplished, however, required a serious investment of resources. There is evidence that their own efforts started decades ago and have been focused and intense (Kim 2018). Nor were the other incursions mentioned above managed on a shoestring and on the run. The SWIFT attack, for example, "showed the patience, skill, and global reach of the hackers" (OFR 2017: 4). In addition, the actual attack on the Russian trading terminal took place a full five months after the initial infiltration (ENISA 2016). Targets were selected, careful reconnaissance was undertaken, information was collected, tools were developed and adapted, and then and only then were attacks made. This requires time, space, money, and expertise, particularly when the target is well aware of its own vulnerability.

This rapidly limits the number of potential state-level attackers in a position to cause real harm to the US financial system. Causing sufficient damage to break down the credit-creation system essential to a healthy economy is a tall order. It is not, however, beyond the ability of nation states like Russia and China. That they each put a high priority on offensive and defensive cyber capabilities is well-known and there is no doubt that they could fund and supply highly-competent teams of hackers taking aim at the banking system (Carr 2012, Lindsay, Cheung, and Reveron 2015, and Reveron 2012). Indeed, it would be surprising to learn that they do not have at least contingency plans along these lines.

https://scholarcommons.usf.edu/mca/vol3/iss2/8
DOI: https://doi.org/10.5038/2378-0789.3.2.1062

That said, the potential for collateral damage and retaliation, not to mention the fact that these states' economies also depend on the availability of finance, suggests that they may be reluctant to take such steps. As Valeriano and Maness argue:

> Even considering our past investigators and theory, we were surprised to find little actual evidence of cyber conflict [between states] in the modern era...Based on our analysis, we find our notion of restraint is a better explanation of cyber interactions than any conception of continuous or escalating cyber conflict. States will not risk war with their cyber capabilities because there are clear consequences to any use of these technologies (Valeriano and Maness 2014: 357).

While recent accusations of Russian interference in the US election may represent evidence to the contrary, it could also be that (assuming the allegations are true) they simply overestimated their ability to hide behind the attribution difficulties inherent to this form of conflict or they viewed the potential fallout as a price worth paying (see for example Berghel 2017 and Fuchs, Kenney, Perina, and VanDoorn 2017). Notwithstanding this possible exception, the data set assembled by Valeriano and Mansess (updated since the publication of referenced article) seems to support their hypothesis that states avoid high-level cyber conflict.[14,15]

Possible Cyber Villains: Terrorists and Activists

Not everyone is so careful, however: "States are not reckless, but terrorists and other cyber activists might not be so restrained" (Valeriano and Mansess 2014: 357). These are precisely the groups from whom we have the most to fear when it comes to destabilizing attacks on the financial system. The relations between two nation states would have to deteriorate significantly for one to undertake the sort of open acts we see from terrorists: kidnaping, assassination, bombing, execution, etc. Furthermore, while states prefer the shadows when undertaking cyber incursions, the whole point of terrorism means that large-scale, well-publicized, dramatic events with collateral damage are very much to their benefit. In addition, the fact that the financial sector is seen as a symbol of America (not unlike the World Trade Center) also makes it a logical and tempting target.

[14] See http://relationsinternational.com/coding-cyber-security-incident-data/

[15] Note, too, that the strong Western reaction to the possibility that Russia may have poisoned Russian ex-patriots in Britain suggests that even if they did risk a high-level confrontation (cyber and otherwise), they may now be reconsidering this strategy (BBC 2018).

All that said, the level of sophistication required for a successful cyber attack lies outside the range normally associated terrorist groups:

> Terrorist organizations can surely find a number of highly trained, intelligent, and computer literate people who are in agreement with their cause. These people can be taught to code, write malware, and hack as well as anyone else can. That will not be enough. They cannot, in a timely manner, develop the kind of large-scale operational capabilities that even a small nation-state possesses. This is what they need to make a truly effective assault on the West in the cyber realm (Bucci 2012: 65).

Therefore, their usual mode of cyber operation is limited to vandalism and denial of service, often carried out by sympathetic hacktivists rather than official operatives (Carr 2012: 15-29). APTs of the sort necessary for a serious attack on the financial sector would require careful planning and a high level of expertise. It is worth recalling that the September 11 attacks were initially proposed in 1996–a full five years before they actually occurred. Planning eventually consumed a half million dollars and at least one dry run (Braun 2011, Eldridge et al 2018, Revesv 2017). Al-Qaeda had to select targets, recruit and train volunteers, and maintain the utmost secrecy throughout.

One of the key reasons they were able to achieve this was the fact that they had a safe and secure base in Afghanistan–and therein lies the key to protecting the financial sector from destabilizing cyber attacks. While cyber security, per se, should obviously be a goal, the most effective defense is simply to deny time and space to bad actors. As Chris Demchak suggests:

> Disruption has the potential to slow wicked actors down. If it is more difficult to operate, adversary actors will need more time to lay in greater amounts of covert leverage than they would normally in order to maintain the economic resources for future exchanges (Demchak 2012: 77).

This is especially true in the current context and disruption (broadly speaking) has long been a key component of US anti-terror policy (Arsenault and Bacon 2015). In that sense it is not a new idea. On the other hand, existing proposals to fight cyber terrorism tend to focus on the establishment of international conventions and cooperation (see for example Cassim 2012, Sofaer et al 2000, and Tehrani, Manap, and Taji 2013). While there is every reason to continue to pursue such avenues, it is unrealistic to believe that these alone will be sufficient. So long as there are locales with power vacuums that terror groups can fill or central governments who turn a blind (or friendly) eye toward bad actors, the potential for destabilizing attacks on the US financial sector exists.

https://scholarcommons.usf.edu/mca/vol3/iss2/8
DOI: https://doi.org/10.5038/2378-0789.3.2.1062

But there is more than one way to disrupt enemy operations. First, it is important to note that "it is less costly to prevent a safe haven from forming in the first place than to try and eradicate it once it has already been established" (Arsenault and Bacon 2015). It is therefore incumbent upon us to act quickly and decisively in those areas that foreign policy analysts have identified as potentially problematic. An ounce of prevention here is worth well more than a pound of cure. Second, where it is too late and bases have been established, every reasonable effort must be made to make the conditions less conducive to quiet, careful planning.[16] Last, where even this is impossible, resources must be devoted to monitoring traffic and tracking suspected incursions. With respect to the latter, it is possible to design systems that allow "analysts to form a total view of the threat by helping them to unify what seems like multiple threats into a single one, thus easing the mitigation effort" (Caglayan et al 2012: 518). Jeffrey Carr also lays out a plan for a cyber early warning model (Carr 2012: 179-89). As suggested above, major attacks are inevitably preceded by months of preparation and these leave a footprint. Attribution is difficult but not impossible. One way or the other, the point here is that the cyber defense of the financial sector is more of a political/military issue than a strictly cyber one.

There are two important wild cards to consider, however: rogue states and criminal organizations. North Korea is not a terrorist organization, per se, but in many respects it has similar goals. Unfortunately, it also offers safe haven with considerable resources and they are sufficiently isolated from the world economy to be insulated from any collateral damage an attack on the financial system may cause. This is a cause for concern, especially at they might act as a sponsor for others. In addition, it has been suggested that terrorist organizations may find allies of convenience in international criminal organizations (Bucci 2012). While they may not possess sufficient cyber resources on their own:

> ...some of these groups have abundant funds and potential access to even more...If a cash-rich terrorist group would use its wealth to hire cybercriminal botnets, or criminal code writers, for their own use, then terrorists could take a shortcut to becoming cyber empowered, thus creating problems for societies dependent on modern communications and the Internet (Bucci 2012: 65).

[16]"Reasonable" is obviously and intentionally ambiguous. The question of whether this is limited to legal, diplomatic channels or may include pre-emptive military operations is not considered here and indeed cannot be in the absence of knowledge of the level and imminence of the threat.

Indeed, while not directly related to creating cyber capabilities, "Cybercriminals have made alliances with drug traffickers in Afghanistan, the Middle East, and elsewhere where illegal drug funds or other profitable activities such as credit card theft, are used to support terrorist groups" (Wilson 2008: 16). This suggests that taking an additional step would not be difficult.

Conclusions

Charles Fox, a cyber-warfare expert for BT Ireland, writes:

> The financial sector in particular is a target for cyber attacks. As transactions change to factor in this new technology, they can leave sensitive data and applications vulnerable to attack. *It's no wonder the International Organisation of Securities Commissions (IOSCO) thinks the next financial crisis will come from cyber space* (emphasis added; Fox 2015: 2).

Quite right, but the financial sector's resilience is such that this is unlikely to be the result of criminal activity alone. Rather, what is required is a targeted and carefully planned and executed campaign. This is well within the capabilities of states like China and Russia, but their motivation to do so is questionable. On the other hand, terrorist groups have much to gain and little to lose. Our attention should therefore be so directed and with special attention to denying them access to the specialized tools and personnel required.

A major, destabilizing strike on the US financial system has the potential to cause a great deal of damage. It has been estimated that not only are output losses from financial crises sizeable, but "a large number of countries never recover their pre-crises growth rates or trends" (Kapp and Vega 2014: 18). Furthermore, the accompanying unemployment has many more costs than most people realize (Tcherneva 2017). On top of all this, it would be an act full of symbolism to anti-Western forces around the world.

https://scholarcommons.usf.edu/mca/vol3/iss2/8
DOI: https://doi.org/10.5038/2378-0789.3.2.1062

References

de Araujo, Pedro, Roisin O'Sullivan, and Nicole B. Simpson. "What should be taught in intermediate macroeconomics?" *The Journal of Economic Education* 44, no. 1 (2013): 74-90.

Arsenault, Elizabeth Grimm and Tricia Bacon. "Eliminating terrorist safe havens: One size does not fit all." Brookings.edu, April 6, 2015. Accessed March 28, 2018.

https://www.brookings.edu/blog/markaz/2015/04/06/eliminating-terrorist-safe-havens-one-size-does-not-fit-all/

Ashford, Warwick. "DDoS is most common cyber attack on financial institutions." ComputerWeekly.com, February 1, 2016. Accessed March 19, 2018.

http://www.computerweekly.com/news/4500272230/DDoS-is-most-common-cyber-attack-on-financial-institutions

Ashford, Warwick. "North Korean hackers tied to cryptocurrency attacks in South Korea." ComputerWeekly.com, January 17, 2018. Accessed March 21, 2018.

http://www.computerweekly.com/news/450433324/North-Korean-hackers-tied-to-cryptocurrency-attacks-in-South-Korea

Ball, Laurence. The Fed and Lehman Brothers. Johns Hopkins Department of Economics Working Paper (2016). Accessed March 3, 2018.

http://www.econ2.jhu.edu/People/Ball/Lehman.pdf

BBC. "Spy poisoning: NATO expels Russian diplomats." BBC.com, March 27, 2018. Accessed March 28, 2018

http://www.bbc.com/news/world-asia-43550938

Berghel, H., 2017. "Oh, What a Tangled Web: Russian Hacking, Fake News, and the 2016 US Presidential Election." *computer*, 50(9), pp.87-91.

Blinder, Alan. "Teaching macro principles after the financial crisis." *The Journal of Economic Education* 41, no. 4 (2010): 385-390.

Boer, Martin and Jaime Vazquez. "Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system." Regulatory Report, International Institute of Finance, September 2017.

https://www.iif.com/publication/regulatory-report/cyber-security-financial-stability-how-cyber-attacks-could-materially

Braun, David Maxwell. "The Original Plans for 9/11." National Geographic Blog, September 7, 2011. Accessed March 28, 2018.

https://blog.nationalgeographic.org/2011/09/07/the-original-plans-for-911/

Bucci, Steven. "Joining Cybercrime and Cyberterrorism: A Likely Scenario." In *Cyberspace and national security. Threats, opportunities, and power in a virtual world*, Derek S. Reveron, ed. Washington, D.C.: Georgetown University Press (2012): 57-68.

Capaccio, Anthony. "U.S. Forces Practice Cyberattacks to Counter North Korean Threat."

Bloomberg.com, January 25, 2018. Accessed March 21, 2018.

https://www.bloomberg.com/news/articles/2018-01-26/u-s-forces-practice-cyberattacks-to-counter-north-korean-threat

Carr, Jeffrey. 2012. *Inside cyber warfare* (second edition). Sebastapol, California: O'Reilly Media, Inc.

Cassim, F., 2012. Addressing the spectre of cyber terrorism: a comparative perspective. PER: Potchefstroomse Elektroniese Regsblad, 15(2), pp.1-37.

Demchak, Chris. 2012. "Resilience, Disruption, and a 'Cyber Westphalia': Options for National Security in a Cybered Conflict World." In *Securing Cyberspace: A New Domain for National Security*, Nicholas Burns and Jonathan Price, editors, Washington, D.C.: The Aspen Institute: 59-94.

Dilanian, Ken. "Watch out. North Korea keeps getting better at hacking." NBCNews.com, February 20, 2018. Accessed March 21, 2018.

https://www.nbcnews.com/news/north-korea/watch-out-north-korea-keeps-getting-better-hacking-n849381

Eggertsson, Gauti B., and Paul Krugman. "Debt, deleveraging, and the liquidity trap: A Fisher-Minsky-Koo approach." *The Quarterly Journal of Economics* 127.3 (2012): 1469-1513.

Eldridge, T.R., Ginsburg, S., Hempel II, W.T., Kephart, J.L., Moore, K. and Accolla, J.M., 2018. *The 9/11 Commission Report: Full and Complete Account of the Circumstances Surrounding the September 11, 2001 Terrorist Attacks*. e-artnow.

ENISA. "Malware infiltrates Russian trading system." European Union Agency for Network and Information Security, February 24, 2016. Accessed March 19, 2018.

https://www.enisa.europa.eu/publications/info-notes/malware-infiltrates-russian-trading-system

Fifield, Anna. "North Korea poised to launch large-scale cyberattacks, says new report." TheWashingtonPost.com, February 20, 2018. Accessed March 21, 2018.

https://www.washingtonpost.com/world/north-korea-poised-to-launch-large-scale-cyberattacks-says-new-report/2018/02/20/7f52196a-160a-11e8-942d-16a950029788_story.html

Fox, Charles. "Breaking the banks: The threat landscape in the financial sector." Dublin: BT Ireland (2015).

https://www.btireland.com/wp-content/uploads/2016/02/BTGS-finance-sector-white-paper-02.pdf

Fuchs, M.H., Kenney, C., Perina, A. and VanDoorn, F., 2017. *Why Americans Should Care about Russian Hacking*. Center for American Progress: Washington, DC, USA.

Harvey, John T. "An Introduction to Post Keynesian Economics: Involuntary Unemployment With Perfectly Flexible Wages and Prices." *The American Economist* 61.2 (2016): 140-156.

Harvey, John T. "An Economics Primer for Cyber Security Analysts." *Military Cyber Affairs* 3(1), 2018 1-42.

https://scholarcommons.usf.edu/mca/vol3/iss2/8
DOI: https://doi.org/10.5038/2378-0789.3.2.1062

Kaplan, Eben. "Tracking Down Terrorist Financing." *Council on Foreign Relations*, 4 April 2006.

https://www.cfr.org/backgrounder/tracking-down-terrorist-financing

Kapp, D. and Vega, M., 2014. Real output costs of financial crises: a loss distribution approach. *Cuadernos de Economía*, 37(103), pp.13-28.

Keynes, John Maynard. *The General Theory of Employment, Interest and Money*, London: Macmillan, 1936.

Keynes, J. M. (1937a). The ex-ante theory of the rate of interest. *The Economic Journal* 47(168), 663-669.

Keynes, J.M., 1937b. The general theory of employment. *The Quarterly Journal of Economics*, 51(2), pp.209-223.

Kim, Sam. "Inside North Korea's Hacker Army." Bloomberg.com, February 7, 2018. Accessed March 21, 2018.

https://www.bloomberg.com/news/features/2018-02-07/inside-kim-jong-un-s-hacker-army

Kopp, Emanuel, Lincoln Kaffenberger, and Nigel Jenkinson. *Cyber Risk, Market Failures, and Financial Stability*. International Monetary Fund, 2017.

Korea Herald. "EDITORIAL: Hacking Provocations." KoreaHerald.com, February 8, 2018. Accessed March 21, 2018.

http://www.koreaherald.com/view.php?ud=20180208000424

Krugman, Paul. "How Did Economists Get It So Wrong?" *New York Times* Sept 2, 2009.

http://www.nytimes.com/2009/09/06/magazine/06Economic-t.html

Lin, Herbert. "Operational Considerations in Cyber Attack and Cyber Exploitation." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, Derek S. Reveron, editor. Washington, D.C.: Georgetown University Press (2012): 37-56.

Lindsay, J.R., Cheung, T.M. and Reveron, D.S. eds., 2015. *China and cybersecurity: Espionage, strategy, and politics in the digital domain*. Oxford University Press, USA.

Minsky, H. P. (1982). *Can it happen again? Essay on instability and finance*. New York: ME Sharpe.

OFR. "Cybersecurity and Financial Stability: Risks and Resilience." Office of Financial Research, Washington: US Treasury Department (February 15, 2017).

https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf

Perlroth, Nicole and David E. Sanger. "Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says." The New York Times, March 15, 2018. Accessed March 19, 2018.

https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html

Raphelson, Samantha. "Report: Russian Hackers Had The Ability To Shut Down U.S. Power Plants." Here and Now Compass, National Public Radio. March 16, 2018. Accessed March 19, 2018.

https://www.npr.org/2018/03/16/594371939/u-s-accuses-russia-of-cyberattacks-on-energy-infrastructure

Reveron, D.S. ed., 2012. *Cyberspace and national security: threats, opportunities, and power in a virtual world*. Georgetown University Press.

Revesv, Rachael. "Saudi Arabia government 'funded dry run' for 9/11, legal documents claim." Independent.uk.com, September 10, 2017. Accessed March 28, 2018.

https://www.independent.co.uk/news/world/americas/911-saudi-government-embassy-dry-run-hijacks-lawsuit-cockpit-security-a7938791.html

Sang-Hun, Choe. "Computer Networks in South Korea Are Paralyzed in Cyberattacks." The New York Times, March 20, 2013. Accessed March 19, 2018.

http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html

Sanger, David E., David D. Kirkpatrick, and Nicole Perlroth. "The World Once Laughed at North Korean Cyberpower. No More." NewYorkTimes.com, October 15, 2017. Accessed March 21, 2018.

https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html

Shiller, Robert J. "How should the financial crisis change how we teach economics?" *The Journal of Economic Education* 41, no. 4 (2010): 403-409.

Sofaer, A.D., Goodman, S.E., Cuéllar, M.F., Drozdova, E.A., Elliott, D.D., Grove, G.D., Lukasik, S.J., Putnam, T.L. and Wilson, G.D., 2000. *A proposal for an international convention on cyber crime and terrorism*. Stanford University, Center for International Security and Cooperation.

Stiglitz, Joseph E. "Rethinking macroeconomics: What failed, and how to repair it." *Journal of the European Economic Association* 9.4 (2011): 591-645.

Tcherneva, Pavlina. "Unemployment: The Silent Epidemic." Levy Economics Institute of Bard College, Working Paper No. 895, August 2017. Accessed March 30, 2018.

http://www.levyinstitute.org/pubs/wp_895.pdf

Tehrani, P.M., Manap, N.A. and Taji, H., 2013. "Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime." *Computer Law & Security Review*, 29(3), pp. 207-215.

Varadhan, Sudarshan. "India bank hack 'similar' to $81 million Bangladesh central bank heist." Reuters, February 19, 2018. Accessed March 19, 2018.

https://www.reuters.com/article/us-city-union-bank-swift/india-bank-hack-similar-to-81-million-bangladesh-central-bank-heist-idUSKCN1G319K

Wislon, Clay. "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress." Washington, D.C.: Congressional Research Service, January 29, 2008. Accessed on March 30, 2018.

https://fas.org/sgp/crs/terror/RL32114.pdf

https://scholarcommons.usf.edu/mca/vol3/iss2/8
DOI: https://doi.org/10.5038/2378-0789.3.2.1062