APPENDIX: A REVIEW OF PAST CYBER INCIDENTS INVOLVING FINANCIAL INSTITUTIONS

This section outlines significant cyber incidents targeting financial institutions around the world from 2011 until December 2016, with the addition of a few selected important incidents between 2007 and 2011. It is noteworthy that there is no public data that any of the incidents involving the manipulation of the integrity of financial institutions' data appear to involve states; this suggests states are exercising restraint so far, except for the disk-wiping attack against South Korean financial institutions allegedly carried out by North Korea, and perhaps the low–level, distributed denial of service (DDoS) attacks targeting Russian financial institutions in December 2016.

The cyber incidents listed in the table below include defacement of websites, DDoS attacks, and intrusions using more sophisticated malware. The targets of the incidents were mainly banks but also one stock exchange and one payment system, and the countries whose financial sectors were hit include Belgium, Brazil, Estonia, Georgia, Lebanon, Russia, South Korea, Ukraine, and the United States. In many cases, it is difficult to know with certainty who perpetrated the attack, but the suspected attackers range from criminals and hacking groups acting independently, to hackers acting under state sponsorship and states themselves. This review was part of the authors' preliminary research and supported the assumption that states already exercise significant restraint in this area compared to what is technically possible.

Table 2: Shorthand for Cyberattacks and Dates

Shorthand	Date
Russian banks DDoS attacks	Late 2016
Bangladesh central bank heist	Early 2016
Belgian National Bank incident	Early 2016
Shanghai Composite Index manipulation (?)	2015–2016
Russian banks theft	Late 2015
Russian currency manipulation	Early 2015
Metel malware attack on Russian banks	2015
Ukrainian Ministry of Finance data breach	Mid 2015
Warsaw Stock Exchange breach	Late 2014
Ukrainian bank data breach	Mid 2014
Carbanak malware attack	2013–2015
Dark Seoul South Korean attacks	Early 2013
JPMorgan data breach	2012–2015
Brazilian banks DDoS attacks	2012, 2014
Brazilian payment system attack	2012–2014
U.S. banks DDoS attacks	2012–2013
Shanghai Composite Index manipulation (?)	Mid 2012
Lebanese Gauss virus infections	2011–2012
South Korean banks attack	Mid 2011
Nasdaq intrusion	Late 2010
Georgian website defacements	Mid 2008
Estonian DDoS attacks	Mid 2007

2016 DDoS Attacks Targeting Russian Financial Institutions

On December 2, the Russian Federal Security Service announced that it had discovered pending cyberattacks intended to impact "a range of major Russian banks" starting from December 5.[30] Servers and command centers purportedly to be used in these attacks were located in the Netherlands and owned by a Ukrainian hosting company named BlazingFast. Its director, Anton Onoprichuk, said he had no information about the asserted attack and that his company was unable to find any malicious data. The Dutch Ministry of Security and Justice said that it was aware its infrastructure could be used for cyberattacks elsewhere, and in a statement noted that "in case . . . a cyberattack does occur on Monday, then it is up to the Russian authorities to decide whether to start an investigation. . . . If desired, they can ask the Dutch investigating authorities for assistance."[31]

On December 9, Rostelecom, Russia's telecom operator, said in a statement that it had blocked DDoS attacks against the five biggest banks and financial institutions in Russia on December 5. They reached a peak volume of 3.2 million packets per second, which is low compared to the volume of other recent DDoS attacks, and the longest lasted a few hours. The statement further noted that part of the DDoS attacks involved a botnet similar to that used in prior weeks against Germany's Deutsche Telekom and Ireland's Eircom, exploiting a vulnerability in home routers.[32]

There was no identification of state actors or perpetrators of the attack, though the Russian Federal Security Service claimed that it was being organized by "foreign intelligence services" and speculation remained that due to the servers' location and ownership, this had been an action on behalf of Ukraine.[33] The Russian Federal Security Service stated that it expected the DDoS attacks to be accompanied by text messages, agitating social network publications, and blog statements about a "crisis in the Russian credit and financial system, bankruptcy and withdrawal of licenses of leading federal and regional banks," and that "the campaign [would be] directed against several dozen Russian cities."[34] Presumably, this would be an attempt to create a run on Russian banks, initiating a financial crisis. No evidence exists that such action, complementary to the DDoS attacks, was attempted.

2016 Bangladesh Central Bank Heist

In February, media reported that hackers had breached the network of the Bangladesh central bank and sent thirty-five fraudulent transfer requests to the Federal Reserve Bank of New York, totaling nearly $1 billion.[35] Four of these fraudulent requests succeeded and the hackers were able to transfer $81 million to accounts in the Philippines, representing one of the largest bank thefts in history.[36] A fifth request for $20 million to be sent to an account in Sri Lanka was stopped when a misspelling of the recipient's name, "Shalika Fandation" rather than "foundation," raised suspicions.[37] The remaining transfers, which totaled somewhere between $850 and $870 million, were also stopped before they could be completed.[38]

The hackers had introduced malware onto the Bangladesh central bank's server and deployed keylogger software that allowed them to steal the bank's credentials for the SWIFT system. The hackers also custom-designed a malware toolkit that compromised SWIFT's Alliance Access system and was designed to cover their tracks.[39] This toolkit allowed them to delete records of transfer requests, bypass validity checks, delete records of logins, manipulate reporting of balances, and stop attached printers from printing transaction logs. Although the malware was custom-designed for the theft, the toolkit could potentially be used against other banks in the SWIFT system running Alliance Access software.

The cybercriminals had monitored the bank's routine activity in order to create money transfer requests that appeared genuine and timed the thefts over the weekend in Bangladesh when the Federal Reserve reached out to confirm the transactions, and then it was the weekend in New York when the Bangladesh central bank employees instructed the Federal Reserve to cancel the transactions.

2016 Belgian National Bank DDoS Attack

On February 22, a hacking group called DownSec Belgium shut down the website for Belgium's National Bank for most of the morning using DDoS attacks.[40] Little information has been reported about the attack, but it followed similar DDoS attacks by the same group against the websites for the Belgian Federal Agency for Nuclear Control, the country's Crisis Center, and Belgium's federal cyber emergency team. DownSec Belgium claims to fight against corrupt government abuses.

2015 Dip in the Shanghai Stock Market (uncertain incident)

Beginning on June 12, the Shanghai Composite Index began to crash, and by June 19 it had fallen by 13 percent.[41] Chinese stock markets continued to fall throughout July and August, and again in January and February 2016.[42] Although there is no public evidence, some have speculated that the sudden crash may have been caused by a cyberattack.[43]

2015 Russian Banks' Thefts From the Banks' Own Customers

There's little information available on this incident currently, but *SC Magazine UK* recently reported that the Russian Central Bank revoked the licenses of three Russian banks in 2015 because an investigation uncovered evidence that current and former bank employees had been using cyberattacks to withdraw money from the accounts of their own clients, as well as to cover up other crimes and violations committed by the banks.[44] The Russian Central Bank reported that in the last quarter of 2015 alone, more than $20 million was stolen from the accounts of clients with what the central bank suspects was the knowledge or direct participation of the banks themselves. The central bank also reported that these hacks were likely the result of huge cuts to the financial industry in Russia over the preceding year, and these cuts had left disgruntled former bank employees willing to collaborate with hackers and left the banks unwilling or unable to shoulder the cost of upgrading their cybersecurity.

2015 Malware Currency Manipulation Through Russian Bank

Russian-language hackers used a virus called the Corkow Trojan to hack into the computer systems of Russian-based Energobank starting in September 2014.[45] They were able to harvest credentials, launch their own trading software, and, on February 27, 2015, they placed more than $500 million in orders at nonmarket rates that caused the exchange rate to swing with extreme volatility between 55 and 66 rubles per dollar for a period of fourteen minutes.[46] Interestingly, it doesn't appear that the hackers made any significant profit directly from the operation itself, although it's possible that they took advantage of their insider knowledge to profit in other markets. It's also possible that this attack was a pilot exercise for future attacks. Energobank has claimed losses of $3.2 million due to the trades.

2015 Metel Malware Attack on Russian Banks

A group of cybercriminals used the previously discovered Metel banking Trojan to steal directly from banks rather than end users. The criminal gang—which is believed to consist of fewer than ten members—used spear phishing emails or browser vulnerabilities to hack into parts of the banks' systems that had access to money transactions, such as the computers used by call center operators or the banks' support teams. Once inside, the Metel malware automated the rollback of ATM transactions. This allowed the criminal group to use cards from the compromised banks to withdraw a virtually unlimited amount of money, because after each transaction the balance on the account automatically reset to the same amount. No infections of this kind have been detected outside of Russia.[47]

2015 Ukrainian Ministry of Finance Data Breach

In May, the pro-Russian hacktivist group CyberBerkut claimed to have hacked into the network of the Ukrainian Ministry of Finance.[48] The group posted what it claimed were documents stolen from the network, demonstrating that Ukraine was unable to service its external debt. The veracity of the group's claims and the means by which they allegedly gained access to the ministry's network remain unknown. See the 2014 Ukrainian data breach entry for more information on CyberBerkut.

2014 Warsaw Stock Exchange Breach

In October, a group claiming to be affiliated with the so-called Islamic State hacked the internal networks of the Warsaw Stock Exchange and posted dozens of login credentials for brokers online.[49] The means by which the group gained access to the exchange's networks are unknown, but they were reportedly able to infiltrate an investment simulator and a web portal for managing the stock exchange's upgrade to a new trading system, as well as render the exchange's website unavailable for two hours.[50] Exchange employees say that the trading system itself was not breached. NATO officials later indicated privately that they believed that the hacking group's claim of being affiliated with Islamic militants was a false flag operation, and that in fact the breach was conducted by APT 28, a group widely believed by security researchers to be affiliated with the Russian government.[51]

2014 Ukrainian Bank Data Breach

In July, the pro-Russian group called CyberBerkut hacked into PrivatBank, one of Ukraine's largest commercial banks, and published stolen customer data on VKontakte, a Russian social media website.[52] The means by which they gained access to the data is unknown. It is believed that they targeted PrivatBank because the bank's co-owner, Igor Kolomoisky, had offered a $10,000 bounty for the capture of Russian-backed militants in Ukraine.[53] CyberBerkut warned PrivatBank customers to transfer their money to state-owned banks. CyberBerkut may have connections to the Russian government, but the relative lack of sophistication of their attacks has led some experts to conclude that official links are unlikely.[54]

2013–2015 Carbanak Malware Attack on Various Banks

A group of criminals used Carbanak malware to attack financial institutions including banks and electronic payment systems in nearly thirty countries. The malware installed a RAT (remote access tool) that allowed the criminals to surveil the banks' daily operations using video feeds and photos over a period of months.[55] The group was then able to order ATMs to dispense cash at terminals and impersonate bank officials to order fraudulent transfers. However, the largest amounts of money were stolen when criminals impersonating bank officers hacked into the banks' accounting systems and manipulated account balances so as to inflate the amount of money available and then transfer the additional money, so that the balance then returned to the original amount. The targeted countries included Australia, Brazil, Bulgaria, Canada, China, the Czech Republic, France, Germany, Hong Kong, Iceland, India, Ireland, Morocco, Nepal, Norway, Pakistan, Poland, Romania, Russia, Spain, Switzerland, Taiwan, Ukraine, the United Kingdom, and the United States.[56]

2013 Malware Attack on South Korean Banks

This was an attack on March 20 that used what's known as Dark Seoul malware against the computer networks of three South Korean banks—Shinhan, Nonghyup, and Jeju—resulting in data deletion and disruptions to ATMs and mobile payment systems.[57] Shinhan Bank's internet banking servers were temporarily blocked for part of the day, leaving customers unable to perform online transactions, while operations at some branches of Nonghyup and Jeju were paralyzed for two hours after the virus erased files on the infected computers. A fourth bank, Woori, reported hacking but suffered no damage. Several Korean media organizations were also hit by the attacks: their computers were frozen but they were able to maintain normal broadcasts.[58] South Korea attributed the attack to North Korea.[59]

2012–2015 Crime Ring Responsible for JPMorgan Data Breach

In August 2014, JPMorgan reported a massive data breach in which hackers had gained access to contact information for over 80 million account holders, representing the biggest data breach of a U.S. financial institution in history.[60] Although there was initial speculation that the Russian government had been involved,[61] federal authorities indicted four men in November 2015 for the data breach, which they said was part of a huge operation that involved hacking into other financial institutions, a stock-pumping scheme, and online gambling operations that in total had netted them $100 million.[62] The criminals used the email addresses they gained through the JPMorgan hack to run a stock price manipulation scheme and also hoped to set up their own brokerage firm using the stolen data to contact potential customers.[63] Although the JPMorgan hack was their biggest, the crime ring had also hacked six other financial institutions, Scottrade, E-Trade, Dow Jones (the parent company that owns the *Wall Street Journal*), another financial news organization, and several online stock brokerages.[64]

2012 and 2014 DDoS Attacks Against Brazilian Banks

In January 2012, the hacker group Anonymous used DDoS attacks to take down the websites of some of the country's biggest banks, which they said was intended to protest corruption and inequality in Brazil.[65] The attacks, which they dubbed #OpWeeksPayment, shut down the websites for Banco do Brasil, Itaú Unibanco, and Bradesco, among others, for hours at a time.[66]

In June 2014, Anonymous launched another series of DDoS attacks, this time to protest the World Cup.[67] The attacks, called #OpHackingCup, took down several Brazilian websites including the Bank of Brazil. Other websites that were targeted included Brazilian government websites, Hyundai Brazil, and the official World Cup site.[68]

2012–2014 Malware Attack on Brazilian Payment System

Cybercriminals used "man-in-the-browser" malware to target Boleto Bancario, a popular Brazilian payment system. The payment system allows businesses to issue paper or online *boletos* (tickets) with a barcode that customers can use to remit money at a bank.[69] The malware injected itself into browsers on nearly 200,000 infected computers, where it was able to intercept and alter legitimate *boletos* so as to route payments into the hackers' own accounts.[70] The attack compromised $3.75 billion in transactions, although it is unclear how much of that money the criminals were able to successfully deposit into their own accounts.[71]

2012–2013 DDoS Attacks on U.S. Financial Institutions

These were two coordinated waves of DDoS attacks against U.S. financial institutions' websites, the first in September–October 2012 and the second in December 2012–January 2013.[72] An Islamic hacktivist group called the Izz ad-Din al-Qassam Cyber Fighters claimed responsibility for the attacks, which they dubbed Operation Ababil,[73] but U.S. government officials have privately indicated to media that they believe Iran is actually responsible.[74] The scale of the attacks was unprecedented in the number of financial institutions hit and the amount of traffic flooding the sites, with one security researcher commenting that "there have never been this many financial institutions under this much duress."[75] Although the group announced the attacks and the targets in advance both times, the banks were unable to defend themselves and access to the websites of many U.S. financial institutions was disrupted, including Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, PNC, Capital One, Fifth Third Bank, BB&T, and HSBC.[76] Defensive and remedial measures have cost the banks millions of dollars to date.[77] Izz ad-Din al-Qassam Cyber Fighters announced two more waves of cyberattacks in 2013, but they appear to have been less effective.[78]

2012 Possible Manipulation of the Shanghai Stock Exchange (uncertain incident)

On June 4, the Shanghai Composite Index opened at a figure of 2,346.98, and fell exactly 64.89 points by close.[79] June 4 is the anniversary of Beijing's infamous 1989 crackdown on student-led protests in Tiananmen Square, prompting many in China to speculate that both figures may have been intended to represent the anniversary of the tragedy.[80] The number 2,346.98 can be read backwards as the year, month, and date, followed by 23 to represent that 2012 marked the twenty-third anniversary of the protests. Similarly, many observers in China speculated that the 64.89 points that the stock market fell that day also represented 6/4/89. The apparent coincidence led to widespread, but unproven, speculation that the index may have been hacked and manipulated in order to produce those numbers. Numerology is very significant in Chinese culture, and Chinese citizens have been known to use numbers as a subtle form of protest in the past.

2011–2012 Gauss Virus Infecting Lebanese Banks

On August 9, 2012, the Russian security firm Kaspersky Lab announced the discovery of the Gauss virus, which is designed to steal data from Lebanese banks—including the Bank of Beirut, EBLF, BLOM Bank, ByblosBank, Fransabank, and Credit Libanais—as well as from users of Citibank and PayPal.[81] Kaspersky's experts concluded that the virus is state-sponsored malware designed by the creators of Stuxnet, Flame, and the Duqu collection of espionage Trojans.[82] More than 2,500 computers belonging to Kaspersky customers have been infected in twenty-five different countries—1,660 of those in Lebanon—although the security firm cautions that the total number of infected machines may number in the tens of thousands.[83]

Once a PC has been infected, the Trojan steals detailed information, including browser history, passwords, cookies, system configurations, and online banking account credentials, and also installs a special font called Palida Narrow, the purpose of which is unknown.[84] Most interestingly, Gauss contains an encrypted payload that security researchers have been unable to decipher, indicating the presence of a significant exploit that the virus's creators clearly considered important to protect.[85] Given that Lebanon serves as a banking hub for the entire Middle East and that the opacity of the country's banks has often been a concern for financial regulators seeking to disrupt terror financing and money laundering, it seems likely that the virus may be designed to monitor and/or disrupt money flows deemed threatening to the sponsor state's national security.[86]

2011 Malware Targeting a South Korean Bank

This incident targeting the banking operations of Nonghyup, a South Korean agricultural cooperative, began on April 12.

The malware initially infected Nonghyup's systems in September 2010 when a subcontractor inadvertently downloaded it onto a laptop, which the attackers used to spread the malware throughout the bank's networks.[87] The attack destroyed the records of some credit card customers and caused a three-day service outage affecting ATMs, online and mobile banking, and credit card usage. South Korea attributed the attack to North Korea.[88]

2010 Nasdaq Intrusion

The intrusion of Nasdaq's networks was first reported in an exclusive *Bloomberg Business* exposé in 2014.[89] In October 2010, the FBI detected an intrusion into Nasdaq's computer servers. The intrusion utilized two zero-day vulnerabilities and resembled malware previously designed by Russia's main intelligence agency, the Federal Security Service. The malware first entered through Nasdaq's Directors Desk, a system that hundreds of companies use to share confidential financial information among board members. Nasdaq's own statement at the time reported that the incursion was limited to that system alone, although *Bloomberg*'s reporting indicated that, in fact, the incursion may have spread more widely through the stock exchange's networks while never accessing the trading platform itself.

The NSA initially believed the malware was capable of causing widespread disruption to Nasdaq's computer networks and of possibly wiping the entire exchange. There were also indications that a large cache of data had been stolen, although investigators had little proof of what exactly had been taken. The CIA later argued that the malware was less destructive than originally believed, and that while it couldn't completely wipe a computer system it could take over certain functions and use them to disrupt the network. The investigators ultimately concluded that the intrusion was primarily designed to steal critical proprietary technology for Russia to imitate or incorporate into its own stock exchanges as part of a push to turn Moscow into a global financial hub. The malware has not been publicly analyzed and *Bloomberg*'s reporting included few details, so further technical information about the malware and its capabilities is unavailable in open-source literature.

2008 Website Defacement During the Russo-Georgian War

Offensive cyber operations against targets in Georgia began on July 20, prior to the outbreak of the war itself, and continued until mid-August when the conflict ceased.[90] This was the first ever combination of offensive cyber operations with kinetic war and was allegedly carried out by the Russian government or Russian hacktivists with ties to the government.[91] On the day that the kinetic war began, websites sprang up with lists of websites to attack, precise instructions, and survey forms for hackers to report their actions after the fact, demonstrating a telling degree of advance preparation and foreknowledge of the beginning of the conflict.[92] The operations consisted of website defacements and DDoS attacks, with targets including the Georgian president's website and other government sites. The only impact on the financial sector was the defacement of the National Bank of Georgia's website.[93]

2007 DDoS Attacks Against Estonia, Including Estonian Banks

A series of coordinated DDoS attacks against Estonian government, bank, university, and newspaper websites began on April 26, lasting for three weeks.[94] During the first week, the DDoS attacks targeted only government and political parties' email servers and websites, while in the second week the target list expanded to include Estonian news websites.[95] In order to bring their websites back online, network administrators had to shut them off to foreign traffic, ironically limiting the ability of Estonia's media to tell the rest of the world what was happening.

The third wave of the attack, which began on May 9, was the heaviest yet and focused on the Estonian banking sector.[96] These attacks forced two major Estonian banks—including Hansabank, the country's largest—to suspend online banking operations while also severing the banks' connection to ATMs and preventing customers from using Estonian debit cards outside the country.[97] This wave of attacks was heaviest on May 9–10, and then slowly decreased thereafter until ending on May 19, when the hackers' botnet contracts appear to have expired.[98]

The attacks were carried out by Russian hacktivists communicating openly on Russian-language chatrooms, where users shared precise instructions on how to conduct the attacks. Estonia accused the Russian government of being responsible for ordering the attacks but couldn't produce definitive proof.[99]