HIGH-TECH HEIST:

CHINESE GOVERNMENT IT VENDORS AND THE THREAT TO US BANKS

MARCH 2021

ROSLYN LAYTON, PHD

TABLE OF CONTENTS

KEY TAKEAWAYS

1. Despite dozens of regulatory policies and a multitude of federal and state agencies charged with overseeing security, cyber attacks on the US financial organizations are increasing in frequency and severity. A cyber attack on a bank can devastate its customers and systems, and a cyber attack on the US Treasury—which SolarWinds came dangerously close to achieving—could bring down the country.
2. The People's Republic of PRC (PRC) is the leading adversary and advanced persistent threat (APT) actor against the United States. It uses cyber attack to conduct theft, espionage, and disruption. The PRC is the only threat actor with a leading information technology (IT) industry which increasingly supplies the IT products and services of US financial organizations.
3. US cyber policy approach which restricts some PRC-owned IT firms but not others is needlessly complex and invites exploitation. Federal policy restricts some purchases from Huawei, Lenovo, Hikvision, and others for security reasons but does not communicate the threats and mitigation in a way that is actionable for banks or end users. Therefore US financial organizations should be proactive to conduct cyber resilience audits, remove elements with vulnerabilities, and adopt NATO's risk reduction strategy to avoid sourcing IT from authoritarian countries. This strategy reduces operational and reputational risks of unwittingly purchasing IT inputs deployed in the repression of human rights.

ROSLYN LAYTON, PhD co-founded China Tech Threat to improve US policy to protect Americans from technological threats from the People's Republic of China (PRC). She is a Visiting Researcher at the Department of Electronic Systems at Aalborg University and Senior Vice President at Strand Consult. She is a Senior Contributor to Forbes. She holds a Ph.D. in business economics from Aalborg University, an M.B.A. from the Rotterdam School of Management, and a B.A. in international service from American University. She can be contacted at roslyn@chinatechthreat.com.

FINANCIAL SERVICES: AN INDUSTRY AT RISK

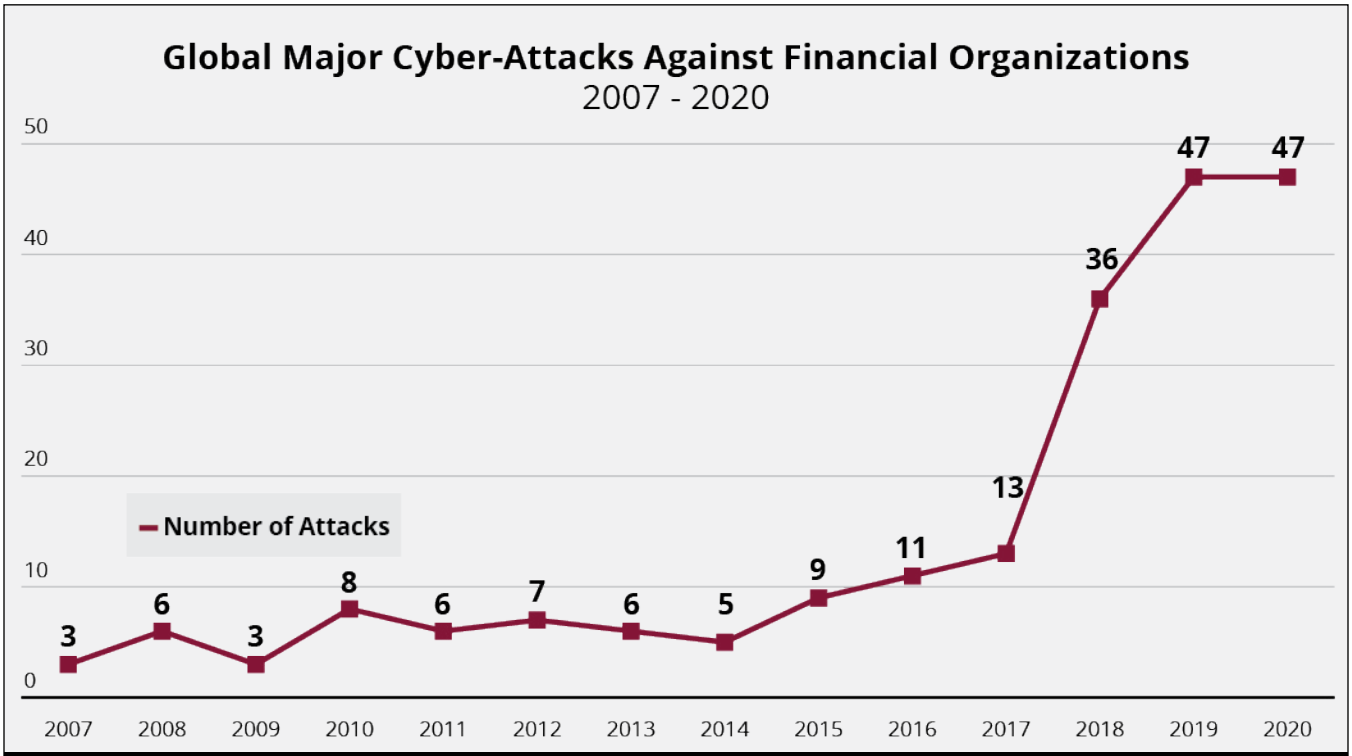
US Financial Organizations: The Number One Target

US financial organizations are the most targeted of any country in significant cyber attacks—and these attacks are escalating in frequency and sophistication, almost tripling between 2017 and 2018. An ongoing survey of publicly available data in English by the Carnegie Endowment for International Peace and BAE Applied Intelligence reports more than 200 major cyber attacks on financial organizations globally between 2007 and 2020.[1] The data is based on publicly available information, and therefore does not include information on attacks which have not been disclosed or not discovered.

Financial organizations in the US are the target for most of the attacks in the study, 55 of 207 (27%) attacks. In half of the attacks against the US, the identity of the attacker is not known. The remaining cases are shared between state and non-state actors, and in sometimes in combination. Data breach and theft resulted in about half of the US attacks. There is also limited information about the method of attack, with it being unknown or unspecified in about one third of the cases. There appears to be no single preferred method of attack.

The next largest target is United Kingdom with 11 attacks. Japan and Russia were each the target of 6 attacks. The PRC also reports just 6 attacks. This is an interesting in that PRC's banking sector is the largest in the world, with assets topping $50 trillion in September 2020.[2, 3] The PRC 's "Big Four" — Industrial & Commercial Bank of PRC Ltd., PRC Construction Bank Corp., Agricultural Bank of PRC Ltd. and Bank of PRC Ltd.—are the world's largest banks, with the country accounting for nine of the world's top 15 banks.[4, 5] The low rate of attack could reflect that attacks on PRC financial institutions are not reported in English. It could also reflect that hacking actors based in the PRC do not target PRC financial institutions.

It is worth reflecting why the US is disproportionately targeted, as the US is an increasingly smaller share of the world's financial sector. The US has just two banks in the top ten,



Data: Carnegie Endowment for International Peace and BAE Systems. Timeline of Cyber Incidents Involving Financial Institutions. FinCyber Initiative, Carnegie Endowment for International Peace. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline, Accessed February 17, 2021

JP Morgan Chase & Co. and Bank of America Corp. Further down the list are Citigroup, Wells Fargo & Co., Goldman Sachs Group, Morgan Stanley, US Bancorp, Truist Financial Corporation, PNC Financial Services Group, Capital One Financial Group, and Bank of New York Mellon. Banks from Japan, France, United Kingdom, and Germany round out the top 100. Without additional data, it is also unclear whether the number of attacks in itself is high; it is possible that existing defenses prevent and deter many more attacks.

"America is grappling with a cyber insurgency and our financial sector is the number one target," Tom Kellermann, who served on a cyber security commission ordered by President Obama, testified before Congress in June 2020. "Although the sector is generally more secure than other industries, it is facing the world's elite hackers, composed of organized crime syndicates and motivated nation-states... Geopolitical tension is manifesting in cyberspace."[6]

A 2015 analysis by Websense Security Labs found that financial services institutions were targeted four times more often than companies in other industries.[7] In 2019, a Boston Consulting Group study found financial services firms may experience 300 times more cyber attacks than other companies.[8]

> "America is grappling with a cyber insurgency and our financial sector is the number one target."
>
> – Tom Kellerman, Cyber Investigations Advisory Board for the United States Secret Service

According to a report by VMWare, cyber attacks against banks spiked 238 percent between February and April of 2020. More than a quarter of cyber attacks that year targeted either the financial sector or healthcare, according to the survey, and third of respondents said they have encountered an attack leveraging island hopping (an attack where supply chains and partners are commandeered to target the primary financial institution) over the past 12 months.[9]

"There has been a significant evolution in the cyber threat facing the global financial industry over the last 18 months as adversaries have advanced their knowledge," a 2017 study commissioned by SWIFT, a global provider of secure financial messaging services, found. "They have deployed increasingly sophisticated means of circumventing individual controls within users' local environments and probed further into their systems to execute well-planned and finely orchestrated attacks."[10]

Interconnectivity Increases Exposure to Paralyzing Attacks

"The threat of cyber security may very well be the biggest threat to the US financial system," J.P. Morgan CEO Jamie Dimon wrote in a 2019 letter to shareholders. "[T]he financial system is interconnected, and adversaries are smart and relentless — so we must continue to be vigilant."[11] As Mr. Dimon notes, the financial services industry is a precarious house of cards. The interconnected nature of the industry means that if one major US bank were upended by a cyber attack, the consequences could be sprawling.

Last year the Federal Reserve Bank of New York issued a report analyzing the impact of a cyber attack on the United States' five major banks. It estimates that if any one of those were to stop making payments, six percent of US banks would breach their end-of-day thresholds, and 38 percent of banks' assets would be affected (excluding the targeted bank).

"[U]ncertainty regarding the nature and extent of the attack could prompt runs to occur in segments of banks' operations that are otherwise unaffected," the report notes. "This reflects the high concentration of payments between large institutions, and the large liquidity imbalances that follow if even one large institution fails to remit payments to its counterparties."[12]

Enormous Data Trove Makes Banks a Valuable Target

The Financial organizations are a prime target not only because of the financial opportunity, but also because of the wealth of personal data they hold. A 2019 report by Bitglass found 75 percent of data breaches in the financial services industry are caused by hacking or malware. The study notes that just six percent of all cyber-security breaches that year were suffered by financial services firms, but those attacks accounted for more than 60 percent of leaked records.[13]

"Given that organizations in the financial services industry are entrusted with highly valuable, personally identifiable information (PII), they represent an attractive target for cyber criminals," said Anurag Kahol, chief technology officer of Bitglass. "Hacking and malware are leading the charge against financial services and the costs associated with breaches are growing. Financial services organizations must get a handle on data breaches and adopt a proactive security strategy if they are to properly protect data from an evolving variety of threats."

US Financial Organizations Should Look to NATO

Cyber attacks against American financial organizations have and continue to increase in frequency and severity, even as US policymakers have added more regulation designed to prevent cyber risk and expanded the federal agencies tasked with cyber-security. US cyber policy, however well-intentioned, is confusing and inconsistent. Some technology makers associated with rogue nations and militaries are restricted, while others are not. Moreover, federal policy is not translated or communicated into actionable items for end users.

Financial organizations must continue to invest in cyber resilience to stay ahead of ever-evolving threats. They should continue to review and monitor systems for vulnerabilities, remove vulnerable products and services and, ideally, avoid vulnerable elements entirely.

For a workable cyber strategy, US should look to NATO which has a simple, defendable policy not to acquire inputs from authoritarian countries. This strategy offers additional benefits of reducing operational and reputational risks from exposure to suppliers engaged in unethical and illicit activities.

Case Study: SolarWinds

The Nightmare Scenario: Black Edge Malware Aimed at the Financial Industry

The SolarWinds episode is a wake-up call for policymakers. Despite best intentions, the complexion of public and private policy instruments is not working to lessen cyber attacks in their frequency or severity. The attack penetrated the US Treasury, coming dangerously close to interrupting the distributions of notes and funds, a process linked to every financial industry in the country. It is not yet known whether and to what degree the attack infiltrated individual banks. The malware itself can remain dormant for months, if not years, evading scanning protocols designed to protect it.

In December of 2020, threat analysis firm FireEye uncovered a global intrusion campaign aimed at the SolarWinds supply chain software and its private and US government clients, including multiple agencies charged with the national security mission of the United States. SolarWinds providers an enterprise network management software platform which helps companies optimize the performance of their computer systems. They gained access to victims via trojanized updates (named Sunburst) to SolarWinds's Orion IT monitoring and management software, meaning that every time the software received an update from SolarWinds, that update then pushed malware through, infecting almost every computer using the update. Once the malware had been activated, it harvested user credentials, exfiltrated classified and proprietary data, and left multiple "stay behinds" to ensure access. The cumulative effects of this attack will likely not be known for years, but at present, it is the most significant successful intrusion in modern history.

SolarWinds exposed and exploited multiple vulnerabilities in the most hardened infrastructure in the world. As such, it has gained attention from researchers, nation state advanced persistent threat (APT) groups, individual hackers/hacktivists, organized crime, and other groups worldwide. These groups look to acquire the tools used for the attack or re-engineer parts of the attack that can be used to conduct additional new attacks. Example of this behavior include the repurposing of Eternal Blue, an offensive tool developed by the US Government to exploit Microsoft systems, which led to "WannaCry" and "NotPetya," two of the most powerful cyber attacks in history.

The possibility of a SolarWinds style attack represents an existential threat to the financial industry. Should any actor, whether it be individual hacker, crime syndicate, nation state or state-sponsored actor, gain access to Sunburst or a variant and then aim it at an institution, that institution would almost certainly experience one or more exploits. Even one successful exploit could result in the loss of customer and account data from private and government individuals, credit information, valuation information and other detailed data. Such a loss of data would cause untold reputational and financial harm.

BUREAUCRACY DOES NOT PROTECT BANKS FROM CYBER ATTACKS

Policymakers have not ignored these developments and have tried to address them through defense and regulatory measures, with many laws, institutions, and protocols established specifically to address cyber threats. However, the success of these efforts appears mixed, as the number of attacks has only increased and become more severe. This comes in addition to significant efforts undertaken by financial organizations themselves to prevent and mitigate cyber attacks.

Financial technology expert Thomas P. Vartanian has charted the rise of US financial regulation and its impact with assiduous documentation in his forthcoming book, *Panic: 200 Years of American Financial Panics: Crashes, Recessions, Depressions, and the Technology That Will Change It All.*[14] He observes of the morass of regulatory agencies and regulation:

> "This highlights the critical problem in the financial services business with multi-organizational cyber-defense systems based on company-by-company, agency-by-agency detection, and defense. Think of the consequences if that were the way the United States deployed its strategic military defense. A large bank like JPMorgan Chase would have to acquire its own supply of ballistic missiles to defend and protect its square block in Manhattan. Traditional approaches being used to defend against cyber threats are somewhat ineffective. Unfortunately, being "somewhat ineffective" in cyberspace can equate to complete ineffectiveness if it takes only one actor probing one vulnerability to cause the collapse of an institution, system, or the economy. The first steps in addressing these issues are elimination of the redundancy in financial oversight and the creation of a reliable and efficient chain of command."[15]

With a nearly $1 trillion annual budget, the US military has some responsibility to address cyber threats, though audits suggest that the Pentagon itself lacks a cyber security culture and hygiene.[16,17,18] In addition, 23 federal departments and agencies are tasked with cyber security responsibilities, including the National Security Council, National Institute of Standards & Technology, the Department of Homeland Security Cyber security & Infrastructure Agency, and the Federal Bureau of Investigation.

Efforts to reform and update federal cyber security frameworks and processes are ongoing,[19] and the Government Accountability Office has warned about a lack of a national strategy and leadership on cyber security.[20] This remains an important question as national defense is the priority job of the government. If the US government cannot protect the people and property of the United States, it fails in its most basic and important responsibilities.

The Extent of Peril Remains Unknown

The cyber security of the US financial organizations is a critically important area of research, but governmental and academic investigations and policy analyses must face the stark reality that cyber attacks are growing faster and larger than the execution of government actions to address them. What elements of US cyber security policy are working, and which aren't, why, and to what degree? Are there policies that unwittingly make the situation worse? If one were to fix the situation, it is difficult to know where to start, what to prioritize and how much it will cost. In any event, regulation does not appear to have reduced the incidence or severity of cyber attack, much less financial cyber war.

Despite significant policymaking, cyber attacks are increasing in frequency, severity, and sophistication.

MUTUALLY ASSURED DESTRUCTION IS NOT A RELIABLE DETERRENCE STRATEGY

Deterrence in Cyberspace Defined

Martin Libiki explains the elements of deterrence in his 2009 report, "Cyber Deterrence and Cyber War."[21] Cyber attacks are asymmetric, in that a single attacker with basic tools can compromise a major system while the cyber-defender must protect a complex network with many components and points of vulnerabilities. In such a situation, it may be difficult to *deny* the attacker the benefits of the attack. However, the cyber-defender can signal a *punishment* so devastating that it deters the cyber attacker. By contrast, the Cold War era relied on deterrence by denial. The United States and Soviet Union engaged an arms race which *denied* the other the benefit of an attack because retaliation and annihilation was assured.

However, cyber-deterrence by punishment has many shortcomings. It is difficult to identify the hacker, and, even if it can be identified, the ability to respond appropriately is limited by speed, time, location, and impact. Declaratory policies and financial regulation do little to deter cyber attackers on banks. Some observe that the internet itself is a source of vulnerability, as it was not designed with security in mind, and ensuring a safer operating environment likely requires re-architecting the internet, which is not a short-term solution.

One unnamed analyst suggests that deterrence of PRC cyber attack comes from the shared interests of US financial organizations with the PRC government to do business. Indeed, the PRC undertook a limited liberalization of its financial sector to allow foreign entry. PayPal, Godman Sachs, JP Morgan, and the leading US credit card companies and the credit rating agencies willingly submit to draconian PRC rules, notably violating US privacy norms, in exchange for pre-determined levels of market access.[22] In any event, doing business in the PRC is subject to the discretion of its authoritarian government, which is hardly a reliable or sustainable promise on which to build cyber defense. Moreover, financial organizations working in the PRC face a host of cyber security issues, not the least of which is Intelligent Tax, a tax-compliance software required by one PRC bank of its foreign customers.[23] The software, dubbed GoldenSpy, installs a hidden backdoor on the customer's corporate network which enables system level privileges separate from the customer's control.

Mutually Assured Destruction

The Hudson Institute's Donald Brennan proposed the term "Mutually Assured Destruction" (MAD) to foil the doctrine of "Assured Destruction" by Robert S. McNamara, US Secretary of Defense in the Kennedy Administration. MAD suggests the premise of deterrence as a means of controlling two or more opponents that would otherwise annihilate each other, if not the earth, through nuclear attack.

MAD is further defined as a Nash equilibrium in Game Theory, as each player is assumed to know the strategies of the other and has no incentive to gain by changing strategy, as the other will follow suit. However, MAD relies on critical assumptions that don't necessarily apply in the cyberworld—for example, that opponents are rational actors, that they have perfect information, and they do not miscalculate.[24] Moreover, the weapons of cyber attack are varied and nuanced, unlike nuclear missiles.

Juan Zarate's paper, "Cyber Financial Wars on the Horizon: The Convergence of Financial and Cyber

Weapons of cyber attack are varied and nuanced, unlike nuclear missiles.

Warfare and the Need for a 21st Century National Security Response" describes the evolution of the practice of defense and national security and the increasing convergence of economic and financial tactics employed by markets, militaries, corporations, and digital battlefields.[25] He notes the irony that the United States has used financial sanctions to pressure bad actors, and now cyber attacks threaten US financial organizations.[26]

Zarate observes, "Our opponents rely on the reliable functioning of international economic infrastructure, and therefore—to date—appear constrained not to conduct systemic or catastrophic attacks on the United States that might collapse international systems or prompt a massive retaliation."

This suggests a fragility of the system itself, its inherent insecurity and its ultimate backup being an attack by the US military. However, there lies a tremendous grey area between what a bank can sustain and the point at which the US military responds. In between, there is tremendous cost and damage experienced on a day-to-day basis, totaling hundreds of billions of dollars annually. It raises the question of whether the job of the US military is only of last and extreme resort. Zarate also suggests privateering, the use of private armies to address and thwart cyber attacks.

Deterrence Is Difficult in Cyberspace

The Cold War was relatively simple in deterrence design and practice pitting two military superpowers. Cyberspace offers a multitude of actors and motivations. Even the basic equation for the United States is magnified by the addition of new countries, like the PRC, North Korea, Russia, and Iran.

In the new book *Shadow Warfare: Cyberwar Policy in the United States, Russia and PRC*,[27] Elizabeth Van Wie Davis examines the policy underpinning of cyber war. She notes that the United States follows Clausewitz's definition of war as a "form of politics by other means" and the notion of "just war," requiring criteria for engaging in conflict. Russian cyber war theory is built on KGB-style tactics of weaponizing information, designed to undermine the authority of opponents in the eyes of their subjects.

The PRC offers yet another strategy based on Sun Tzu's notion of fighting without having to go into battle. Deception is critical to the Chinese understanding of war and ensuring that its opponents never have the full measure of its capabilities, fooling opponents into thinking the PRC has more capability when it does not, and vice versa.

> The PRC marries the teachings of Sun Tzu with technological leapfrogging, and, as such, is likely conducting cyber-warfare against the US financial industry without its knowing.

The United States and the PRC approach war in different ways. The United States believes that war must be declared, explicit, and conform to "just war" requirements. The PRC wants to fight without engaging in battle, will engage in significant deception to obfuscate their capabilities and will leverage technological leapfrogging to their advantage. The PRC desires preeminence in certain industries, and it is unclear how its vision for financial services could impact a strategy toward US banks.

The Maoist development model seeks self-sufficiency and domestic supply for key technological inputs. This contrasts with traditional liberal economic models, in which nations specialize in different sectors and freely trade with one another, maximizing the efficiency and comparative advantages of each other. The PRC desires to dominate strategic global industries while ensuring it can supply the world markets with finished goods and services. This strategy includes a component of technology development fulfilled by "build, buy, or steal" tactics.

Cyber attacks on banks are perpetrated for economic, financial, political and military reasons. Like old fashioned bank robbers, some hackers want money and currency. This is a key for North Korea, a country frozen out of world markets because of sanctions.[28] A recent DOJ indictment cites the PRC's enabling role to North Korea in $1.3 billion of global financial crimes.[29]

The PRC hacking world is an ever-changing mix of official, military, and civilian actors, which may engage in state-sponsored, freelance, or independent attacks.[30] Hired hackers may be allowed to profit personally from their exploits. Sophisticated "cyber-thieves" seek to acquire information about businesses, individuals, customer lists/databases, technologies, and intellectual property. This information can be resold as enterprise information and/or mined for intelligence purposes.

In other cases, attackers may want to make political statements, as "hacktivists" use internet activism and other computer-based techniques as form of civil disobedience to promote a political agenda or social change. For example, while the Chinese military employs many hackers, the country also has many independent hackers which undertake hacks for patriotic and other political reasons. Chinese military hackers may desire cyber intrusion for espionage purposes.

Notably, banks in all nations are targets for cyber attacks, but the US financial industry offers distinct features in that it contains the information and assets of many important, strategic companies and high net worth individuals, in addition to being home to leading financial exchanges and actors in financial innovation.

Technological Globalism: The PRC Is the Winner that Takes All

Another explanation of the status quo is that globalization, whether wittingly or unwittingly, rewards the PRC more than others to the detriment of democratic, multi-lateral governance models. Leading military intelligence expert James Mulvenon, considered a front runner to lead the Department of Commerce's Bureau of Industry and Security, explains this in a recent article, "A World Divided: The Conflict with Chinese Techno-Nationalism Isn't Coming – It's Already Here."[31]

Mulvenon attributes the reign of technological globalism[32,33] to the "Davos set" and the gurus of the Fourth Industrial Revolution, who want a borderless world organized by transnational social media platforms and supply chains.[34] However "global" this regime claims to be, its supply chain and IT actors are increasingly national, located in and controlled in a single place: the PRC (albeit with some product assembly in Taiwan).

Mulvenon characterizes today's world as two different technological ecosystems—one dominated by PRC firms either implicitly or explicitly controlled by the mercantilist Chinese state,[35] and the other an "amorphous technological environment" comprising the Organization for Economic Co-operation and Development countries and their associated firms (yet, increasingly penetrated by PRC actors). Notably, the PRC model is increasingly authoritarian, while the other evolves policy and regulation to accommodate democratic norms and expectations.

"The edges where these two spheres meet are now in a persistent site of conflict, with the demands of global interconnectivity and supply chains chafing against a range of trade and export security concerns," Mulvenon observes.

The US Department of Commerce's Bureau of Industry and Security is key to addressing the problem. "As a core mission, the bureau should begin by placing the interests of the United States, its long-term economic vitality, and its people ahead of the near-term financial interests of Silicon Valley, Wall Street, and other multinationals, which are not always aligned with US interests," notes Mulvenon. He calls for the United States to protect its innovation from being acquired by the PRC's state-owned enterprises and national tech champions by way of export controls, economic sanctions, merger reviews by the Committee on Foreign Investment in the United States (CFIUS) and offensive investment in American research & development.

INFORMATION TECHNOLOGY AS A WEAPON: SYSTEMIC RISK OF EMBEDDED COMPONENTS

Advanced Persistent Threats (APTs)

As the name suggests, an Advanced Persistent Threat (APT) attack is a sophisticated, sustained attack meant to infiltrate a network and conduct long-term operations, such as spying or data exfiltration. APT can also refer to a group of attackers like APT1 and APT2 which refers to specific groups in the PRC military. Unlike an opportunistic cyber attack – in which the perpetrator seeks to "get in and get out" for some immediate payoff – an effective APT will sidestep a system's security and remain undetected for a prolonged period.

Once inside, an APT may implement malware, access sensitive information or plant backdoors that allow future access. Unlike other attacks, APTs require patience and generally significant resources to identify a target and instigate the attack. These hacks can span months and even years and are designed to avoid detection by resembling authentic code or programs within a network. As such, many APTs are nation states with that staying power and resources to conduct a attack over time.

The prolonged nature of an APT attack allows the attacker to spy on the target and collect large swaths of data. The leading sources of APTs against the United States are the PRC, North Korea, Russia and Iran. Of these, only the PRC has a key position in the production of information technology, enabling it to install physical and virtual backdoors into its products and services. The use of technology to surveille and exfiltrate information in the PRC is already practiced and documented.

For example, in 2010, Lee Chieffalo who managed the operations center for the US Marines in Iraq, testified, "A large amount of Lenovo laptops were sold to the US military that had a chip encrypted on the motherboard that would record all the data that was being inputted into that laptop and send it back to China. "That was a huge security breach. We don't have any idea how much data they got, but we had to take all those systems off the network."[36] It is naïve to think that the PRC would not retain this capability in its exports of information technology.

This is a particular concern for malware embedded in IT hardware, as demonstrated in tiny unauthorized circuits embedded on server motherboards in the controversial and still unresolved Supermicro case. The situation illustrates that products from US firms can be compromised by third-party suppliers in the PRC. Reporting from Bloomberg in 2018[37] and 2021[38] includes corroboration from multiple US intelligence and security officials who allege that the People's Liberation Army in concert with a Chinese subcontractor attached a tiny chip into thousands of motherboards intended for US companies.

> "A large amount of Lenovo laptops were sold to the US military that had a chip encrypted on the motherboard that would record all the data that was being inputted into that laptop and send it back to China."
>
> – Lee Chieffalo, Data Chief, US Marine Corps

Once installed in servers, these stealth backdoors could open networks to hackers. The attack was reported to have impacted at least 30 companies, including a major bank, Apple and Amazon Web Services. Apple subsequently ripped and replaced 7,000 servers, and Amazon terminated a related supplier in PRC.

"Hardware hacks are more difficult to pull off and potentially more devastating, promising the kind of long-term, stealth access that spy agencies are willing to invest millions of dollars and many years to get," the 2018 Bloomberg article stats. "In Supermicro, PRC's spies appear to have found a perfect conduit for what US officials now describe as the most significant supply chain attack known to have been carried out against American companies."

Jay Tabb, who served as Executive Assistant Director of the FBI's national security branch from 2018 to 2020, observes:

> Supermicro is the perfect illustration of how susceptible American companies are to potential nefarious tampering of any products they choose to have manufactured in China. It's an example of the worst-case scenario if you don't have complete supervision over where your devices are manufactured. The Chinese government has been doing this for a long time, and companies need to be aware that China is doing this… And Silicon Valley in particular needs to quit pretending that this isn't happening."[39]

APT attacks have accelerated in the wake of the Coronavirus pandemic. The PRC has coordinated "aggressive" disinformation campaigns to build support for their own systems of governance, which is part of a broader long-term campaign, notes a new report by Recorded Future and the Insikt Group.[40] Chinese APTs have targeted healthcare and biotech industries to steal business information and gain an economic advantage.[41]

Indeed, the PRC is reported to employ thinly-veiled threats to purchase Chinese products—or else.[42] In December 2019, *Berlingske* reported on a recording it obtained featuring the PRC ambassador to Denmark telling leaders of the Faroe Islands that if a purchase of Huawei equipment was declined, China would drop its "free trade agreement" with the archipelago, threatening the export of fish to China.[43] Later that month the PRC ambassador to Germany threatened "consequences" if the Germany government excluded Huawei.[44] In Brazil, PRC representatives reportedly demanded that the country stop restrictive measures on Huawei for the delivery of COVID-19 vaccine supplies to proceed.[45] *The New York Times* reported that to counter reservations about Huawei expressed by IT buyers in Belgium (headquarters to NATO and the European Union), a covert pro-Huawei, Chinese disinformation influence campaign used fake Twitter accounts, amplified by Huawei officials, to spread positive articles about the company and negative views of Belgium's 5G policy.[46]

"State-sponsored hacking is the biggest threat to our financial sector because of the capacities that they can bring to bear," noted Jamil Jaffer, the founder and executive director of George Mason University's National Security Institute. "They have almost unlimited resources…you just can't beat a nation state at their own game."[47]

Even if the embedding of backdoors into its products alone was not sufficient risk, PRC employs a host of other practices that should cause IT buyers to reconsider. These include its stated policy of Civil-Military Fusion, its stated policies for cyber security

espionage and surveillance, and its influence and intelligence practices through internet governance, international standards bodies and trade associations.

Civil Military Fusion

The PRC has a stated practice of "Civil-Military Fusion," in which any economic input in the PRC can be commandeered for military purposes.[48] This contrasts with the American notion that there are strict boundaries between the military and civic life, and ultimate civilian control over the military, which is enshrined in the US Constitution. The PRC's army is a political one, and there is not the separation of government and military as it is understood in the United States. Technology is central to implementing the strategy of "Unrestricted Warfare,"[49] the transcendence of traditional methods of war to vanquish adversaries like the United States through "asymmetrical" or multidimensional means, including economic, financial, political, biological, and cyber means.

"Made in China 2025" is the PRC's official plans to dominate ten strategic technological industries globally in the future.[50] The plan is a type of "techno-nationalism" and includes designation of a series of national champions that deliver the PRC's goals in targeted industries like information technology, robotics, aerospace, green energy, medicine, semiconductors and more.[51] The PRC's national tech champions receive the spoils of state support, forced joint venture, strategic acquisition, tech transfer, theft and cyber-espionage. Examples include Huawei in telecom equipment, Lenovo in laptops, Inspur in servers, Tecent in social networks, Alibaba in ecommerce, Baidu in search, and Semiconductor Manufacturing International Corporation (SMIC) in semiconductors.[52]

Under Mao's concepts of the "people's war," every citizen is recruited as a part of the long-term revolutionary struggle. For example, hackers are celebrated in Chinese popular culture.[53] The ascendancy of General Secretary Xi Jingping is associated with a revival of Maoist notions and strengthening of the "Chinese Dream,"[54] the vision of "comprehensive national power"[55] and global supremacy by 2049, 100 years from the founding of the modern Chinese state.

Following Mao's notion of a people's war that encompasses all of society and technological inputs, the United States can expect that the PRC will leverage its citizens and technologies anywhere at any time to conduct a war that its adversaries may not recognize is going on. This presents a predicament for the use of PRC technologies in the banking environment, given their ability to process, store, and transmit data.

Control of Cyberspace

Recent laws adopted in the PRC increase the risk of doing business with any PRC IT company. For example, the PRC's 2016 Internet Security Law asserts the country's sovereignty over cyberspace, authority over all internet products and services made in PRC, and obligations of PRC producers of internet products and services to the PRC.[56]

The United States can expect that the PRC will leverage its citizens and technologies anywhere at any time to conduct a war that its adversaries may not recognize is going on.

The PRC's 2017 National Intelligence Law compels any Chinese subject to spy on behalf of the state. As such, the PRC's information communication technology (ICT) firms can be compelled to collect data or conduct surveillance on any piece of technology at any time for any reason anywhere.[57] Customer information collected on Chinese devices anywhere can also brought to the PRC. Indeed, many contracts with Chinese IT providers stipulate as much. However, data need not be taken out of the United States to be available to the PRC.

A sample of publicly available contracts negotiated between state governments and PRC IT vendors shows that information transmitted on the vendors' equipment is now subject to collection, transfer, processing and inspection by the vendor, and could be transferred to any country where the vendor does business and to any entity with whom it works. For example, one basic sales agreement with technology manufacturer Lenovo notes that data can be transferred across international borders to any country where Lenovo operates.[58] This includes the PRC where the data is subject to PRC law and where US and EU expectations of privacy and data protections are not necessarily honored.

Notably, US law does not prohibit data transfer out of the United States even if it can go to the Chinese government. Recent US attempts to restrict certain Chinese apps like TikTok reflect the danger of Americans' sensitive data being transferred to the PRC, as the apps regularly supply such information to Chinese authorities as part of the PRC's Social Credit System. In recent years, the Committee on Foreign Investment in the United States (CFIUS) intervened on many transactions like MoneyGram, StayNTouch, Grindr and PatientsLikeMe because sensitive personal and financial data, as well as geolocation, HIV status, sexual orientation and medical information, was at risk of falling into the hands of the PRC.[59]

Other Influence and Intelligence Practices

Under General Secretary Xi, the PRC has entered a period of consolidation of its domestic internet controls and has pursued internationalizing those norms on the world stage.[60] Significantly, this includes a new design for the Internet presented to the United Nations, which includes embedded backdoors already incorporated into existing technology by Huawei and others.[61] Importantly, this includes replacing the notion of an open, borderless Internet in which information can flow freely with "internet sovereignty," computer systems designed for social control and government surveillance. Notably, these controls and protocols are embedded in the smart and safe cities solutions offered by PRC firms.[62,63]

The PRC has entered a period of consolidation of its domestic internet controls and subsequently has pursued internationalizing those norms on the world stage.

To set agendas and drive technological discussions, the PRC has secured leadership positions in U.N. agencies like the International Telecommunication Union, World Summit on the Information Society, and the Internet Governance Forum and related events, like the World Summit on Information Technology. As meticulously detailed in *Hidden Hand: Exposing how the Chinese Communist Party Is Reshaping the World,* when the PRC talks of making global organizations more "inclusive," it means increasing their acceptance of authoritarian regimes and giving Chinese Communist Party (CCP) values equal weight as democratic ones.[64]

Authors Clive Hamilton and Mareike Ohlberg detail how the PRC has succeeded in "Sinicizing" the U.N. by building up support for third world nations to gain a seat on the U.N. Human Rights Council, with the goal of subsequently perverting the notion of universal human rights to one that accepts "human rights with Chinese characteristics." The PRC consistently scores as one of the worst violators of human rights and "makes technology central to repression" according to Human Rights Watch.[65]

University of Virginia PRC Internet policy expert Aynne Kokas describes how the PRC influences standard-setting through national regulation, industrial dominance and multi-stakeholder organization.[66] Notably, Chinese law requires many IT firms to insource data to the PRC, storing it on government-run servers. Meanwhile the PRC exports its laws through the practices deployed by PRC companies abroad. A type of "cyber-sovereignty,"[67] the PRC's policy is an extension of asserted territorial rights, like those to the South China Sea and Taiwan Straits, to the digital domain. Literally hundreds of Chinese government and military affiliated organizations are part of technology standards organizations and trade associations, such as the International Standards Organization, the International Electronic Commission, 3GPP, IEEE, Wi-Fi Alliance, the ORAN Alliance and others.

The PRC has proposed a new design for the Internet to the United Nations which includes embedded backdoors already incorporated into existing technology by Huawei and others.

Many companies and countries practice industrial espionage, but the PRC takes it to the next level with the integration of diplomatic, academic and military intelligence, as well as seemingly ordinary professionals, students and tourists, which enable the theft of intellectual property and valuable information.[68] A cursory review of the cases brought by the US Department of Justice's China Initiative demonstrates many common and banal situations in which one would never suspect major IP theft to take place.[69] As such, the salespeople, account and product managers, and technicians of PRC IT firms are uniquely placed to gather information when they service their customers.

The Foot in the Backdoor: Vulnerable IT from Chinese Government-Owned and Affiliated Firms

The PRC has an IT industry that sells hardware, software, and other applications to banks, and these technologies are gaining market share. Major US action has restricted Huawei, ZTE, Hikvision and others, but there is nothing to stop other state-owned and state-affiliated companies from installing backdoors on any piece of PRC hardware. In fact, the Chinese government may require it.

Consequently, the PRC's enormous position in the IT manufacturing market gives it many long-term advantages to conduct infiltration (it has the blueprints of all its products and the legal authority to do so), supply chain attacks (embedding malware in products), human intelligence (learning about customers, participating in US trade associations) and social engineering. This vulnerable technology is not just the high-end servers and data centers, but also consumer-off-the-shelf (COTS) products like laptops, printers and webcams.

Called one of the scariest hacks and vulnerabilities of 2019,[70] an audit by the US Department of Defense (DoD) Inspector General detailed more than $30 million in purchases by government contractors who unwittingly purchased PRC brands Lenovo and Lexmark with known cyber security vulnerabilities because DoD failed to provide a blacklist of items or to review IT purchases.[71]

Supply chains are vulnerable to threats that may turn out to be more significant in the long term: Chips could be intentionally compromised during the design process *before* they are even manufactured. If placed into the design with sufficient skill, these built-in vulnerabilities would be extremely difficult to detect during testing. And they could be exploited months or years later to disrupt or exfiltrate data from a system containing the compromised chip. Such a scenario was detailed in *Ghost Fleet: A Novel of the Next World War*, which describes the grounding of US fighter jets because of compromised circuits produced in the PRC. The Central Intelligence Agency issued a complimentary review of the book.[72]

These risks extend to emerging technology. Consider the situation with facial recognition technology, which enables physical access into facilities and authentication of users for accounts, payments and ATMs. However important and valuable the technology may be, its development and deployment in PRC government surveillance and repression of human rights has sparked a global backlash, from the Department of Commerce Entity List designation of Megvii for use of the technology on Uighur Muslims in Western PRC[73]; condemnation by Human Rights Watch,[74] and variety of bans and regulation proposed by Council of Europe on the development of facial recognition.[75]

Plans for Megvii's IPO were scuttled, implicating the involvement of investment banks Goldman Sachs, Citigroup, and JP Morgan.[76] In December 2020, the Washington Post described a chilling patent application by Huawei, the Chinese Academy of Sciences and Megvii for the identification of Uighur Muslims at large and subsequent reporting to the police.[77] The widespread deployment of Megvii's Face++ technology in consumer products such as smartphones made by Huawei, Xiaomi and Vivo; "smile-to-pay" terminals by Alibaba; and laptops made by Lenovo (in addition to Lenovo seeding Face++ development[78]) have caused reputational headaches for many organizations unwittingly engaged with these products.[79]

PROACTIVE STEPS FOR THE FINANCIAL INDUSTRY

Prudent Risk Management in an Uncertain World

Cyber attacks against the US financial services sector are growing, both in number and sophistication. The consequences could not be greater. A successful attack on even one major US bank could have a ripple effect across the industry, disrupting commerce and creating widespread turmoil. A larger attack could bring the US economy to a halt. Less catastrophic but equally alarming, cyber security vulnerabilities in the financial organizations could jeopardize sensitive personal data and allow adversaries to spy on American consumers.

Despite best intentions, US policy has not succeeded in meaningfully reducing the frequency or severity of cyber attack. Rationalizing US cyber policy across a multitude of domains into a coherent and consistent whole is politically difficult, if not impossible. Sadly, US banks and financial service providers cannot rely solely on the government to combat state-sponsored cyber-security threats.

US banks and financial service providers cannot rely solely on the government to combat state-sponsored cyber-security threats.

Financial organizations are naturally risk-averse organizations, and many have employed proactive strategies to secure their networks and will likely need to continue, if not redouble, these efforts.

Moreover, ever-growing financial regulation seeks to criminalize banks for data breaches, even if the breaches originate from rogue nations that the US military ostensibly guards against.

The growing volume of cyber attacks coupled with greater technology manufacturing occurring outside the United States—75 percent of the world's mobile phones and 90 percent of its PCs are made in the PRC[80]—creates a computing landscape rife for cyber attacks. As noted above, those threats should be especially alarming for financial services companies, which are targeted with greater sophistication and with greater frequency.

Below are four proactive steps for the financial organizations to secure their cyber infrastructure:

1. Don't wait for policymakers to fix the problem
2. Conduct cyber resilience audits
3. Remove elements with cyber vulnerabilities
4. Adopt a secure cyber sourcing strategy

Don't Wait for Policymakers to Fix the Problem

It can take years for government agencies to recognize and act to prevent the infiltration of vulnerable equipment into the marketplace. For example, in 2012, the US House Permanent Select Committee on Intelligence issued guidance that US government systems and government contractors not use Huawei or ZTE telecommunications equipment or component parts, but the DoD did not take action until five years later when Congress prohibited the DoD from acquiring this equipment. Even when the US government identifies cyber risks, there is no systematic communication to the public or end users to inform them of risks. The National Vulnerabilities Database is a valuable resource to list technical shortcomings in information technology and provides a status report on efforts to repair them. However, it does not say whether a product is safe for purchase.

Moreover, US cyber policy is a mix of many measures, instruments and agencies. It may come from different branches of government with different applications, objectives and legal authority. These policies may be inconsistent,

incoherent and/or incomplete. For example, some IT firms with ties to the PRC military and government are restricted, but not others. This creates policy cleavages to exploit—firms lobby policymakers to weaken regulation, and IT buyers, seeing inconsistency, don't take US policy seriously.

Financial organizations need to take proactive steps because when a cyber attack hits, the firm, not the US government, will be held responsible. Moreover, the firm may even be prosecuted for the data breached in the attack, even if the attack is state-sponsored and impossible for the firm to prevent or mitigate. Very simply, government regulation cannot stop a cyber attack. Due diligence in selecting technology can—or at least, stands a better chance.

Conduct Cyber Resilience Audits

Resilience is toughness or the capacity to recover quicky. The frontline of cyber defense for the financial services industry must be companies' own cyber resilience audits, including the security of informational technology and its flow through people, processes and products in the organization. Financial organizations need to acquire and develop reliable intelligence. They must proactively monitor and review their systems, identify vulnerabilities and take steps to reduce and remedy vulnerability.

The Carnegie Endowment for International Peace offers a website for Cyber Resilience for financial organizations and an associated capacity-building tool box. Guides, checklists, and worksheets are offered for banks' boards of directors, CEOs and management, security leaders, employees, customers and third-parties. These are tailored for small, medium, and large organizations as well as offered in seven languages.

Remove Elements with Cyber Vulnerabilities

Much cyber security discourse and practice are focused on software and applications, and while important, these can compel organizations to de-emphasize hardware and physical facilities security. As the Supermicro case illustrates, the motherboard hardware products of a US firm were compromised by third-part supplier linked to the PRC military to enable a sophisticated attack across the network of an organization.

This revelation reportedly led to Apple removing thousands of servers and Amazon terminating a supplier in China.

"Hardware represents a gaping and exploitable hole in the current approach to cyber security. The varied means of attack illustrate how hardware-level vulnerabilities can be exploited to completely sidestep software-based security countermeasures," notes John Villasenor.[81]

Financial organizations must realize that hardware like phones, laptops, cameras and servers are not stand-alone devices that can be isolated from a network. They are extremely complex machines with their own embedded software, which can integrate and infiltrate larger networks and systems. Banks must bring the same vigilance to hardware as software. As such, banks must also be prepared to remove products, services and other elements which present cyber risk and vulnerability.

> "Hardware represents a gaping and exploitable hole in the current approach to cyber security... [H]ardware-level vulnerabilities can be exploited to completely sidestep software-based security countermeasures."
>
> – John Villasenor, Former Nonresident Fellow, Center for Technology Innovation, Brookings Institution

Adopt a Secure Cyber Sourcing Strategy

The adage that an ounce of prevention is worth a pound of cure holds true for cyber security. Rather than remove vulnerable IT, an organization is better off not to acquire it in the first place. Financial organizations can be prudent to employ proven risk reduction strategies by eliminating information technology products, services and relationships from countries known for vulnerability.

One such strategy is deployed by the NATO Support and Procurement Agency (NSPA). Its procurement strategy is based upon the pillars of consolidation of bids to achieve value for money, competition among countries, and the traditional public procurement principles of integrity, transparency, and equal treatment.[82] To uphold these principles, NATO does not contract or subcontract with authoritarian, communist countries because, by definition, they cannot maintain these standards. As such NATO has enshrined a policy that it will not engage with the PRC, Cuba, Laos, North Korea and Vietnam.[83] In practice, NATO only sources from NATO countries.

US companies—particularly financial organizations with a wealth of enterprise and personal data—must be vigilant to select IT equipment and services that are made in democratic nations. This may require additional diligence and greater spending more for security.

A secure cyber sourcing strategy has the benefit of reducing operational and reputational risk, which increases with the size and profitability of a bank.[84] Notably, the risk management agenda has evolved from the control of technical factors to the demonstration of governance and responsibility.[85] Moreover, banks increasingly respond to regulators, the media and other external actors that grade their reputations risk.

US companies—particularly financial organizations with a wealth of enterprise and personal data—must be vigilant to select IT equipment and services that are made in democratic nations.

CONCLUSION

Prudent Risk Management in an Uncertain World

Cyber attacks against the US financial services sector are growing, both in number and sophistication. The consequences could not be greater. A larger attack could bring the US economy to a halt. American companies in every industry—but especially financial organizations—must be proactive in addressing these threats, rather than relying on government agencies.

As cyber threats continue to evolve and grow, so too must companies' cyber defenses. There is no silver bullet but following best practices and continually auditing their systems and equipment will help financial organizations stay ahead of attackers—and better protect US financial organizations assets, reputation, and shareholder value.

ENDNOTES

1 Carnegie Endowment for International Peace and BAE Systems. Timeline of Cyber Incidents Involving Financial Institutions. FinCyber Initiative, Carnegie Endowment for International Peace. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline, Accessed February 17, 2021

2 BNEditor, "Total Assets of Chinese Financial Institutions Exceed $50 Trillion as of Q2 2020," China Banking News (blog), September 15, 2020, https://www.chinabankingnews.com/2020/09/15/total-assets-of-chinese-financial-institutions-exceed-50-trillion/.

3 Reuters Inc, "Chinese Banks Dispose of $467 Billion Soured Assets in 2020, Pressure Remains | The Guardian," accessed January 27, 2021, http://www.theguardian.pe.ca/business/reuters/chinas-banking-sector-disposed-of-467-billion-soured-assets-in-2020-statement-543757/.

4 Pablo de la Riva, "Cybercriminals in Financial Sector: The Culprits behind the Keystrokes," accessed January 27, 2021, https://www.buguroo.com/en/blog/cybercriminals-in-the-financial-sector-understanding-the-culprits-behind-the-keystrokes.

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

6 Miller Maggie, "Financial Firms Facing Serious Hacking Threat in COVID-19 Era," Text, The Hill, June 16, 2020, https://thehill.com/policy/cybersecurity/503051-financial-firms-facing-serious-hacking-threat-in-covid-19-era.

7 Maria Korolov, "Banks Get Attacked Four Times More than Other Industries," CSO Online, June 23, 2015, https://www.csoonline.com/article/2938767/report-banks-get-attacked-four-times-more-than-other-industries.html.

8 "Cyber Risk and the US Financial System: A Pre-Mortem Analysis - FEDERAL RESERVE BANK of NEW YORK," January 2020, https://www.newyorkfed.org/research/staff_reports/sr909.

9 Tom Kellermann, "'Modern Bank Heists' Threat Report Finds Dramatic Increase in Cyberattacks Against Financial Institutions Amid COVID-19," VMware Carbon Black (blog), May 15, 2020, https://www.carbonblack.com/blog/modern-bank-heists-threat-report-finds-dramatic-increase-in-cyberattacks-against-financial-institutions-amid-covid-19/.

10 "The Evolving Cyber Threat to the Banking Community" (Swift, November 2017), https://www.swift.com/swift-resource/176276/download?language=en.

11 Hugh Son, "Jamie Dimon Says Risk of Cyberattacks 'May Be Biggest Threat to the US Financial System,'" CNBC, April 4, 2019, https://www.cnbc.com/2019/04/04/jp-morgan-ceo-jamie-dimon-warns-cyber attacks-biggest-threat-to-us.html.

12 "Cyber Risk and the US Financial System: A Pre-Mortem Analysis" Federal Reserve Bank of New York." June 2020 https://www.newyorkfed.org/research/staff_reports/sr909

13 "More than 60% of All Leaked Records Exposed by Financial Services Firms," Security, December 16, 2019, https://www.securitymagazine.com/articles/91412-more-than-60-of-all-leaked-records-exposed-by-financial-services-firms?v=preview.

14 Thomas P. Vartanian. 200 Years of American Financial Panics: Crashes, Recessions, Depressions, and the Technology That Will Change It All (Prometheus Publishing (2021).

15 Thomas P. Vartanian, "Country, banking long overdue for cyberdefense upgrade," American Banker, December 39, 2020, https://www.americanbanker.com/opinion/country-banking-long-overdue-for-cyberdefense-upgrade.

16 "DOD Completes First Full Financial Statement Audit; Findings Will Directly Benefit Readine," US DEPARTMENT OF DEFENSE, November 16, 2018, https://www.defense.gov/Newsroom/Releases/Release/Article/1692138/dod-completes-first-full-financial-statement-audit-findings-will-directly-benef/.

17 U. S. Government Accountability Office, "Cybersecurity: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene," no. GAO-20-241 (April 13, 2020), https://www.gao.gov/products/GAO-20-241.

18 "Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases," Department of Defense Office of Inspector General, July 26, 2019, https://www.dodig.mil/reports.html/Article/1920236/audit-of-the-dods-management-of-the-cybersecurity-risks-for-government-purchase/.

19 "Cyberspace Solarium Commission," accessed November 25, 2020, https://sites.google.com/solarium.gov/cyberspace-solarium-commission.

20 General Accountability Office. "Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy," GAO-20-629 (September 22, 2020), https://www.gao.gov/products/GAO-20-629.

21 Libicki, Martin C. *Cyberdeterrence and cyberwar*. RAND corporation, 2009.

22 Nicholas Lardy and Tianlei Huang. "Despite the rhetoric, US-China financial decoupling is not happening." Peterson Institute for International Economics. July 2, 2020. https://www.piie.com/blogs/china-economic-watch/despite-rhetoric-us-china-financial-decoupling-not-happening

23 Brian Hussey. "The Golden Tax Department and the Emergence of GoldenSpy Malware." TrustWave June 25, 2020. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-golden-tax-department-and-the-emergence-of-goldenspy-malware/

24 Sreyas Misha, "When Mutually Assured Destruction Breaks Down," Stanford, April 16, 2018, http://large.stanford.edu/courses/2018/ph241/misra1/.

25 Juan Zarate, "FDD | The Cyber Financial Wars on the Horizon," FDD, July 7, 2015, https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/publications/Cyber_Financial_Wars.pdf.

26 Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare*, 1st edition (New York: PublicAffairs, 2013).

27 Elizabeth Van Wie Davis, *Shadow Warfare: Cyberwar Policy in the United States, Russia and China* (Rowman & Littlefield Publishers, 2021).

28 Chanlett-Avery, Emma, et al. *North Korean Cyber Capabilities: In Brief*. Congressional Research Service, 2017.

29 "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe: Indictment Expands 2018 Case that Detailed Attack on Sony Pictures and Creation of WannaCry Ransomware by Adding Two New Defendants and Recent Global Schemes to Steal Money and Cryptocurrency from Banks and Businesses while Operating in North Korea, China. Department of Justice. February 17, 2021. https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and

30 Howlett, William IV, "The Rise of China's Hacking Culture: Defining Chinese Hackers" (2016). Electronic Theses, Projects, and Dissertations. 383. https://scholarworks.lib.csusb.edu/etd/383

31 James Mulvenon. A World Divided: The Conflict with Chinese Techno-Nationalism Isn't Coming – It's Already Here War on the Rocks. January 28, 2021. https://warontherocks.com/2021/01/a-world-divided-the-conflict-with-chinese-techno-nationalism-isnt-coming-its-already-here/

32 Ostry, Sylvia, and Richard R. Nelson. *Techno-nationalism and techno-globalism: Conflict and cooperation*. Brookings Institution Press, 2000.

33 Rodrik, Dani. The globalization paradox: democracy and the future of the world economy. WW Norton & Company, 2011.

34 Klaus Schwab. Fourth Industrial Revolution: What is means, how to respond. World Economic Forum. January 14, 2016. https://www.weforum.org/focus/fourth-industrial-revolution

35 Jude Blanchette. "From "China Inc." to "CCP Inc.": A New Paradigm for Chinese State Capitalism." China Leadership Monitor. December 1, 2020. https://www.prcleader.org/blanchette

36 USA v. Ehab Ashoor. | [2010] | US District Court, Southern District of Text, Houston Division | No. H-09-CR-307| https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/r9dKMMM0Gi5I/v0

37 Jordan Robertson and Michael Riley. "The Big Hack: How China Used a Tiny Chip to Infiltrate US Companies."Bloomberg. October 4, 2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

38 Jordan Robertson and Michael Riley. "The Long Hack: How China Exploited a US Tech Supplier." Bloomberg. February 12, 2021. https://www.bloomberg.com/features/2021-supermicro/

39 Ibid

40 "Follow the Money: Qualifying Opportunism Behind Cyberattacks During the COVID-19 Pandemic," *Recorded Future* (blog), January 22, 2021, https://www.recfut.com/opportunism-behind-cyberattacks-during-pandemic/.

41 Alex Marquardt, Kylie Atwood, and Zachary Cohen, "US Formally Warns China Is Launching Cyberattacks to Steal Coronavirus Research," CNN, May 14, 2020, https://www.cnn.com/2020/05/13/politics/us-china-hacking-coronavirus-warning/index.html. See the statement issued the by the FBI https://www.fbi.gov/news/pressrel/press-releases/peoples-republic-of-china-prc-targeting-of-covid-19-research-organizations

42 Mihir Sharma, Bloomberg Opinion, "China's Bullying Tactics Will Only Unite Its Foes," https://www.bloomberg.com/opinion/articles/2020-11-19/china-s-trade-pressure-on-australia-will-likely-fail

43 Simon Kruse and Line Winther. "Banned recording reveals China ambassador threatened Faroese leader at secret meeting." December 10, 2019. Berlingske. https://www.berlingske.dk/internationalt/banned-recording-reveals-china-ambassador-threatened-faroese-leader

44 Scott Bicheno. China Threatens Germany Over Huawei. December 16, 2019. Telecoms.com https://telecoms.com/501405/china-threatens-germany-over-huawei/

45 Renato Santino, "Government May Release Huawei for 5G to Receive Supplies for Vaccines," Olhar Digital (blog), January 22, 2021, https://olhardigital.com.br/en/2021/01/21/coronavirus/release-of-supplies-for-vaccines-to-brazil-may-pass-by-allowing-huawei-no-5g/

46 Adam Satariano, "Inside a Pro-Huawei Influence Campaign," The New York Times, January 29, 2021, sec. Technology, https://www.nytimes.com/2021/01/29/technology/commercial-disinformation-huawei-belgium.html.

47 Maggie Miller, "Financial firms facing serious hacking threat in COVID-19 era," The Hill, June 16, 2020, accessed February 8, 2021, https://thehill.com/policy/cybersecurity/503051-financial-firms-facing-serious-hacking-threat-in-covid-19-era.

48 "2020 Report on Military and Security Developments Involving the People's Republic of China,"US Department of Defense, September 2020, https://www.defense.gov/Newsroom/Releases/Release/Article/2332126/dod-releases-2020-report-on-military-and-security-developments-involving-the-pe/

49 Qiao, L., Wang, X., & Santoli, A. (2002). Unrestricted warfare : China's master plan to destroy America. Panama City: Pan American Publishing Company.

50 Made In China 2025. (2016). Retrieved from http://www.gov.cn/zhuanti/2016/MadeinChina2025-plan/index.htm?_sm_au_=iVVbN6VM35s7Nk2501TfKK3Qv3fc

51 "China's Technonationalism Toolbox: A Primer | US- CHINA | ECONOMIC and SECURITY REVIEW COMMISSION," March 28, 2018, https://www.uscc.gov/research/chinas-technonationalism-toolbox-primer.

52 Yang, Y., & Liu, N. (18, September 18). SMIC scores mainland China's biggest listing in a decade. Retrieved from https://www.ft.com/content/6a87d390-fdad-43c7-8ff9-c99f3b94294c

53 "Freedom for Authoritarianism: Patriotic Hackers and Chinese Nationalism," The Yale Review of International Studies (blog), October 12, 2014, http://yris.yira.org/essays/1447

54 Jinping, X. (2014). THE CHINESE DREAM OF THE GREAT REJUVENATION OF THE CHINESE NATION. https://www.amazon.com/CHINESE-DREAM-GREAT-REJUVENATION-NATION/dp/7119086960

55 Angang, H.; Honghua, M. (n.d.). The Rising of Modern China: Comprehensive National Power and Grand Strategy (Rep.). Tsinghua University.

56 "网络安全法 (草案) 全文," June 1, 2017, http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm. Translation: Rogier Creemers, Paul Triolo, and Graham Webster, "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," New America, June 29, 2018, http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

57 "网络安全法 (草案) 全文." Translation: https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf

58 China Tech Threat. "Stealing from the States: China's Power Play in IT Contracts." March 2020. https://chinatechthreat.com/wp-content/uploads/2020/02/CTT-Report-Stealing-From-States-Chinas-Power-Play-in-IT-Contracts.pdf

59 China Tech Threat. CFIUS' Growing Power to Protect American Security from China Tech Threats: Examining TikTok and Lenovo. June 2020. https://chinatechthreat.com/wp-content/uploads/2020/06/CFIUS-Paper-062420_.pdf

60 Negro, Gianluigi. *Internet in China: From Infrastructure to a Nascent Civil Society*. Palgrave Macmillan, 2017.

61 Madhumita Murgia and Anna Gross, "China and Huawei Propose Reinvention of the Internet," March 27, 2020, https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2.

62 Yau Tsz Yan, "Smart Cities or Surveillance? Huawei in Central Asia," August 7, 2019, https://thediplomat.com/2019/08/smart-cities-or-surveillance-huawei-in-central-asia/.

63 Samantha Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion," October 14, 2019, https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion.

64 Hamilton, Clive, and Mareike Ohlberg. *Hidden hand: exposing how the Chinese Communist Party is reshaping the world*. Simon and Schuster, 2020.

65 "World Report 2021: Rights Trends in China," Human Rights Watch, January 13, 2021, https://www.hrw.org/world-report/2021/country-chapters/china-and-tibet. "World Report 2020: Rights Trends in China's Global Threat to Human Rights," Human Rights Watch, January 3, 2020, https://www.hrw.org/world-report/2020/country-chapters/global.

66 Kokas, Aynne, Cloud Control: China's 2017 Cybersecurity Law and its Role in US Data Standardization (July 26, 2019). Available at SSRN: https://ssrn.com/abstract=3427372

67 Schneier, Bruce (2015). Data and Goliath: *The Hidden Battles to Collect Your Data and Control Your World.* New York: W.W. Norton & Company

68 Peter Mattis and Matthew Brazil, *Chinese Communist Espionage: An Intelligence Primer* (Naval Institute Press, 2019).

69 "Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018." Department of Justice. https://www.justice.gov/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related Accessed February 17, 2021.

70 Catalin Cimpanu, "The Scariest Hacks and Vulnerabilities of 2019," ZDNet, October 28, 2019, https://www.zdnet.com/article/the-scariest-hacks-and-vulnerabilities-of-2019/.

71 Joseph Marks, "China Tech Threat's Special Report on the DoD IG's Inquiry," *China Tech Threat* (blog), August 22, 2019, https://chinatechthreat.com/dod-inspector-general-report/.

72 August Cole, "Cole's 'Ghost Fleet' Reviewed by CIA's 'Intelligence in Public Media,'" *Atlantic Council* (blog), March 29, 2016, https://www.atlanticcouncil.org/insight-impact/in-the-news/cole-s-ghost-fleet-reviewed-by-cia-s-intelligence-in-public-media/.

73 "Addition of Certain Entities to the Entity List," Federal Register, October 9, 2019, https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list.

74 Maya Wang, "The Robots Are Watching Us," Human Rights Watch, April 6, 2020, https://www.hrw.org/news/2020/04/06/robots-are-watching-us.

75 "Consultative Committee of the Convention for the Protection Og Individuals with Regard to the Automatic Processing" (Convention 108, January 28, 2021), https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3.

76 Joshua Franklin Zhu Julie, "Goldman Evaluating Role in China's Megvii IPO after US Blacklist," Reuters, October 9, 2019, https://www.reuters.com/article/us-megvii-ipo-goldman-sachsgoldman-sachs-idUSKBN1WN2DT

77 IPVM offers a timeline of the reporting and analysis of the patent incident: ipvideomarket, "Huawei / Megvii Uyghur Alarms," IPVM, 44:00 500, https://ipvm.com/reports/huawei-megvii-uygur.

78 "Lenovo Capital and Incubator Group Created to Advance Core Technology Investments," Lenovo StoryHub (blog), May 6, 2016, https://news.lenovo.com/pressroom/press-releases/lenovo-capital-and-incubator-group-created-to-advance-core-technology-investments/.

79 "Facial Recognition Specialist Megvii Plans Share Sale," BBC News, August 26, 2019, sec. Technology, https://www.bbc.com/news/technology-49473583.

80 John Naughton, "The Tech Giants, the US and the Chinese Spy Chips That Never Were...or Were They?" *The Guardian*, October 13, 2018, https://www.theguardian.com/commentisfree/2018/oct/13/tech-giants-us-chinese-spy-chips-bloomberg-supermicro-amazon-apple

81 John Villasenor. Compromised By Design? Securing the Defense Electronics Supply Chain. Brookings Institution, November 23. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/Villasenor-Securing_the_Defense_Electronics_Supply_Chain.pdf

82 NATO Support and Procurement Agency. "Key principles of NSPA procurement" https://www.nspa.nato.int/business/procurement. Accessed February 5, 2021.

83 Clause 7. Special Areas. NSPA Operating Instruction. March 19, 2019. https://www.nspa.nato.int/resources/site1/General/business/procurement/General%20info/OI-4200-01-EN.pdf

84 Franco Fiordelisi, Maria-Gaia Soana, Paola Schwizer. The determinants of reputational risk in the banking sector, Journal of Banking & Finance, Volume 37, Issue 5, 2013. https://doi.org/10.1016/j.jbankfin.2012.04.021.

85 Power M, Scheytt T, Soin K, Sahlin K. Reputational Risk as a Logic of Organizing in Late Modernity. Organization Studies. 2009;30(2-3):301-324. doi:10.1177/0170840608101482

www.chinatechthreat.com