Financial Weapons of War

Tom C.W. Lin
Article

Financial Weapons of War

Tom C.W. Lin†

INTRODUCTION

Finance may be the most powerful weapon of war.¹ It moves armadas, armies, and squadrons. It funds troops and artillery. It endows suicide bombs and improvised explosive devices.² It pays for special forces and mercenaries. It underwrites cease-fires and purchases surrenders. Finance is the weapon that makes all other weapons of war possible.³

† Associate Professor of Law, Temple University Beasley School of Law. Many thanks to Kenneth Anderson, Derek Bambauer, Gary Brown, Rebecca Crootof, Onnig Dombalagian, Jeffrey Dunoff, Charles Dunlap, Adam Feibelman, Richard Gordon, Sean Griffith, Duncan Hollis, Eric Talbot Jensen, Ann Lipton, Duncan MacIntosh, Gregory Mandel, Shu-Yi Oei, David Post, Sasha Radin, Steven Sheffrin, Peter Spiro, Harwell Wells, and conference and workshop participants at the Murphy Institute at Tulane University, Seton Hall University School of Law, the 2015 International Committee of the Red Cross Workshop on Autonomous Legal Reasoning at Temple University, 2014 Ontario Securities Commission Dialogue, and the 2015 National Business Law Scholars Conference for their invaluable comments, exchanges, and insights. Additionally, I am grateful to Thomas Helbig, Leslie Minora, and George Tsoflias for their extraordinary research assistance. Copyright © 2016 by Tom C.W. Lin.


2. See, e.g., JOHN ROTH ET AL., NAT’L COMM’N ON TERRORIST ATTACKS UPON THE U.S., MONOGRAPH ON TERRORIST FINANCING: STAFF REPORT TO THE COMMISSION 19–30 (2004) (describing the financing necessary for terrorist activity, including Central Intelligence Agency estimates that al Qaeda spent approximately $30 million annually in the lead up to the September 11th attack).

3. See, e.g., S.C. Res. 2255, ¶ 6, 18, U.N. Doc. S/RES/2255 (Dec. 22, 2015) (alluding to the importance of financing in warfare); FIN. ACTION TASK FORCE,
This Article is about the financial weapons of war, their growing importance in national affairs, and their wide-ranging effects on law, finance, and society. This Article offers an early, broad examination of the realities of modern financial warfare. This Article descriptively and normatively explores the new financial theater of war, analyzes the modern arsenal of financial weapons, highlights emerging legal and policy concerns, and proposes key recommendations for current and future financial warfare.

While policymakers, analysts, and scholars have long been studying the respective, evolving fields of modern finance and modern warfare, there has been surprisingly little meaningful legal scholarship on the crosscutting realities of modern financial warfare. Drawing on a rich legal literature that spans the laws of war, finance, and cyberspace, this Article seeks to fill


4. See ZARATE, supra note 1, at ix–xiii (describing various efforts made by the United States in financial warfare following September 11, 2001).


7. See, e.g., CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS (J. Ohlin et al. eds., 2015); SHANE HARRIS, @WAR: THE RISE OF THE MILITARY-
This understudied, underappreciated—yet critically important—legal intersection of war and finance.

This Article has two chief objectives. First, this Article strives to offer an original preliminary understanding of the expansive effects of financial weapons of war and modern financial warfare. Second, building on that new working understanding, this Article aims to identify and address larger, emerging normative consequences for law, finance, and society given contemporary realities relating to financial warfare. The objectives of this Article are largely conceptual in nature; as such, detailed discussions of issues pertaining to legislative language, policy execution, and political economy will be the focus of future work. In pursuit of its two chief objectives, this Article is mindful of a longstanding view that generally perceives economic and financial hostilities as activities that fall below the threshold of warfare, but it argues for a different perspective under certain circumstances in light of developments in recent history. Jointly, this Article’s binary objectives do not seek to advance an elegant, comprehensive theory of financial warfare. Instead, this Article aspires to provide an early, working conceptual blueprint for thinking and acting anew about modern financial warfare. Such an endeavor to draw the dynamic and fast-evolving architecture of modern financial warfare will necessarily be a preliminary work-in-progress. Nonetheless, it is a blueprint that must be sketched and studied, for the financial weapons of war have become too consequential and too important to ignore or wait for a later time.

This Article unfolds this blueprint in four parts. Part I provides a general layout of the modern financial theater of war. It describes the modern financial infrastructure as a globalized, high-tech, American-centric system. It then identifies systemic risks, discrete vulnerabilities, and a lineup of potential adver-

---

8. See infra Part III.A.
9. See infra Part I.
saries in this financial theater of war. Part I provides a sweep-  
ing survey of the emerging financial battlefield.  

Moving from general to specific, Part II highlights particu-  
lar armaments of financial warfare. Rather than provide an  
exhaustive catalog of financial weapons, it offers a broad inven-  
tory of the financial weapons of war. It classifies the financial  
weapons of war as analog weapons and cyber weapons. It ac-  
counts for traditional weapons like economic sanctions, anti-  
money laundering regulations, and banking restrictions, as  
well as digital weapons like distributed denial-of-service at-  
tacks, data manipulation hacks, and destructive intrusions.  

It explains how these analog and cyber weapons are used in cur-  
rent conflicts with al Qaeda, Iran, the Islamic State of Iraq and  
Syria (ISIS), North Korea, Russia, and Syria. Part II examines  
and explains the utility and evolution of these weapons in mod-  
ern financial warfare.  

Part III contends with new concerns. It asserts that the fi-  
nancial weapons of war present critical challenges for traditio-  

tal laws and norms relating to financial hostilities, cyberattacks, and non-state actors. It argues that certain tra-  
ditional rules that governed finance and war in the past are ill-  
suited for a fundamentally different present, and a dramatical-  

dy distinct future. It does so respectful of conventional norms  
and laws governing wars and armed conflicts, but mindful of  
the need to adapt to new realities. Part III grapples with core  
concerns posed by the financial weapons of war to certain fund-  
mamental principles governing war and finance.  

Part IV offers new pathways. It proposes three pragmatic  
policy recommendations that should be undertaken in the near  
term response to modern financial warfare while larger issues  
remain unresolved by global policymakers. It advocates for in-  
novative cybersecurity incentives, advanced technological  
stress tests, and comprehensive financial war games to better  
prepare for threats in the financial theater of war. Part IV  
suggests immediate forward steps to be seriously considered  
while larger policy and legal disagreements are being deliber-  
ated and debated by global policymakers.  

This Article ends with a brief conclusion. It reminds of the  
growing and emerging dangers of the financial weapons of war.  
And it signals, with hope and optimism, the possibility of tam-
ing the savageness of financial weapons, safeguarding the economy of the homeland, and promoting the integrity of the global financial system.

I. A NEW THEATER OF WAR

The new theater of war is the modern financial infrastructure. This new theater of war presents an extremely valuable battle space for our adversaries because they may be able to plunder funds for their efforts and cause widespread financial panic and crisis simultaneously. Unlike previous wartime theaters, the financial theater of war is less defined by geography and more by its critical functions, assets, and liabilities. The financial theater of war presents new risks, threats, and vulnerabilities for modern warfare posed by a cast of familiar and unfamiliar antagonists.

A. THE MODERN FINANCIAL INFRASTRUCTURE

The modern financial infrastructure serves as a new battlefield in contemporary warfare. In this new battlefield, instead of bombs and bullets, the weapons of choice are financial and economic in nature. This new battlefield is the result of advances and developments in information technology, geopolitics, and financial regulation over the last half century. The

13. See, e.g., ZARATE, supra note 1, at ix ("Over the past decade, the United States has waged a new brand of financial warfare, unprecedented in its reach and effectiveness."); John Seabrook, Network Insecurity, NEW YORKER, May 20, 2013, at 64 (reporting on the growing number of cyberattacks on the American financial infrastructure).

14. See Kelly A. Gable, Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent, 43 VAND. J. TRANSNAT’L L. 57, 84 (2010) ("The international financial system is such a large target for cyberterrorists because of the substantial rewards that cyberterrorists stand to gain—from stealing large amounts of money to fund other terrorist acts, to crushing the global economy by shutting down the international financial system, to more subtly affecting international markets by eroding consumer confidence.").


16. See ZARATE, supra note 1, at xi (characterizing financial warfare as one "defined by the use of financial tools, pressure, and market forces to leverage the banking sector, private-sector interests, and foreign partners in order to isolate rogue actors from the international financial and commercial systems and eliminate their funding sources").

17. See ERIC J. WEINER, THE SHADOW MARKET: HOW A GROUP OF
modern financial infrastructure is an international, high-tech, American-centric theater of commerce and conflict.

First, the modern financial infrastructure is an international, interdependent system of intermediation.\textsuperscript{18} Finance connects the world as a source of capital for good and ill. It connects nation-states, private businesses, terrorist organizations, rogue syndicates, allies, and adversaries.\textsuperscript{19} Contemporary financial participants and products operate in a complex, expansive global network that connects and crosses institutions, industries, individuals, and instruments across the world.\textsuperscript{20} Nation-states invest in one another through sovereign wealth funds and other vehicles. Commercial banks, investment banks, exchanges, pension funds, sovereign funds, mutual funds, and many other financial institutions are all interconnected like never before, coexisting in an expansive financial ecosystem with numerous linked participants and products.\textsuperscript{21} For instance, J.P. Morgan Chase, the largest American banking institution, serves as a nexus for a panoply of counterparties through a wide-ranging array of services and products that in-


\textsuperscript{19} See \textit{Zarate, supra} note 1 ("Money binds the world—now more than ever. It has always been a source of power for nations, companies, and people. It continues to be the lifeblood for terrorist organizations, criminal syndicates, and rogue regimes.").


cludes investment banking, commercial banking, lending, market-making, trading, clearing, custodial servicing, and prime brokering. In fact, the U.S. Treasury Department’s Office of Financial Research found that J.P. Morgan Chase was the most interconnected bank in the world and had more cross-jurisdictional activity than any other bank in 2015. Additionally, financial institutions play an important role in the global market for commodities that are essential to many non-financial sectors of the economy like oil, aluminum, and coal.

In recent years, financial institutions like Morgan Stanley and Goldman Sachs physically held such large stakes of commodities like oil and aluminum that they could significantly influence the global prices for those commodities.

While the financial system has long been global in nature, geography matters much less now. In previous eras, the successes and failures of one institution, state, or instrument were more readily contained and captured by borders and boundaries. In present times, the ripples caused by one institution, state, or instrument move so much farther, quicker, and stronger than before. This was made bluntly evident during the recent financial crisis when volatility in the American markets for collateralized debt obligations and mortgage-backed se-

25. See Omarova, supra note 6, at 311–23 (discussing the holdings and influence of financial institutions in connection with commodities markets).
26. See Austin Murphy, The Making and Ending of the Financial Crisis of 2007–2009, in LESSONS FROM THE FINANCIAL CRISIS: CAUSES, CONSEQUENCES, AND OUR ECONOMIC FUTURE 125, 128 (Robert W. Kolb ed., 2010) (“The failure of just one large financial institution might lead to the failure of one or more other institutions that would then spread to yet more financial institutions in a contagion that was feared might end in the collapse of the entire financial system.”); Judge, supra note 6, at 659 (arguing that new linked products in the modern financial system generate new sources of systemic risk); David M. Serritella, High Speed Trading Begs High Speed Regulation: SEC Response to Flash Crash, Rash, 2010 U. ILL. J.L. TECH. & POLY 433, 437 (noting the potential perils emanating from “the interconnectivity of financial markets and their participants, as well as increased interconnections between securities and their derivatives”).
securities caused significant stress on the global financial system.\textsuperscript{27} The more recent sovereign debt crisis in Europe, and its cascading effects around the world, offers even more credence to the notion of a global, interdependent modern financial infrastructure.\textsuperscript{28}

Second, in addition to being a global, interdependent system, the modern financial infrastructure is also a high-tech system driven by new information technology and new communications technology.\textsuperscript{29} Complimentary advances in technology and regulation over the last five decades have remade the inner and outer workings of the financial system.\textsuperscript{30} Technological advances made computing power and capacity exponentially better, faster, smaller, cheaper, and more readily accessible for everyone, including financial institutions.\textsuperscript{31}

\begin{itemize}
\item \textsuperscript{28} See, e.g., Clive Crook, Who Lost the Euro?, BLOOMBERG BUSINESSWEEK, May 28, 2012, at 10; James Kanter, After Talks, Eurozone and Greece Fail To Settle Differences over Debt, N.Y. TIMES, Feb. 12, 2015, at B3.
\item \textsuperscript{29} See RAY KURZWEIL, THE AGE OF SPIRITUAL MACHINES: WHEN COMPUTERS EXCEED HUMAN INTELLIGENCE 70 (1999) (“Not only were the stock, bond, currency, commodity, and other markets managed and maintained by computerized networks, but the majority of buy-and-sell decisions were initiated by software programs.”); MICHAEL LEWIS, FLASH BOYS: A WALL STREET REVOLT 3–10 (2014); Markku Malkamaki & Jukka Topi, Future Challenges for Securities and Derivative Markets, in 3 RESEARCH IN BANKING AND FINANCE 359, 382 (Iftekhar Hasan & William C. Hunter eds., 2003) (“At the end of [the] 1990s, between 30% and 40% of all U.S. securities were channeled through the Internet and about 15% of all the U.S. equity trades were done on-line.”).
\item \textsuperscript{31} See NICHOLAS CARR, THE SHALLOWS: WHAT THE INTERNET IS DOING TO OUR BRAINS 83 (2011) (“[T]he price of a typical computing task has dropped by 99.9 percent since the 1960s.”); Donald C. Langevoort & Robert B. Thompson, “Publicness” in Contemporary Securities Regulation After the JOBS Act, 101 GEO. L.J. 337, 347 (2013) (“Today, liquidity is now much more possible outside of traditional exchanges. In the new millennium, cheap information
today contains more computing power than all of NASA during the first lunar mission. Along a similar timeline, regulatory developments like Regulation Alternative Trading System, Regulation National Market System, and decimalization spurred the growth of electronic communication networks and alternative trading platforms that linked financial markets all across the globe. The net effect of the convergence of advances in technology and regulation is a high-tech, modern financial infrastructure.

In today’s financial marketplace, smart machines powered by complex algorithms run much of finance. Financial tasks that previously required human teams to exert hours, days, and weeks of effort have gradually been replaced by artificial intelligence, algorithmic models, and supercomputers that per-
form those tasks exponentially faster, cheaper, and in a more user-friendly manner. High-frequency trading programs powered by artificial intelligence trade billions of dollars in securities and commodities across the world in fractions of a second without any human assistance in public markets, as well as in private dark pools. Autonomous supercomputers assist financial institutions in assessing risk and managing assets. Online brokerages and automated wealth managers empower retail investors to participate in finance like never before. Thus, it should come as little surprise that a financial institution, J.P. Morgan Chase, has recently been estimated to employ “more software developers than Google and more technologists than Microsoft.”

In sum, the modern financial infrastructure is a high-tech system where information technology is at the core and foundation of the entire framework.

Lastly, in addition to being international and high-tech, the modern financial infrastructure is an American-centric system. Despite globalization and the emergence of other nation-states, the United States stands as the lone superpower in the world. While geography may matter less in finance today, in terms of financial influence and economic clout, America remains second to none. Our 2014 annual gross domestic product of $17.42 trillion leads the world. Our currency is the reserve currency of the world, and the most trusted investment during

38. See Lin, supra note 18, at 653–54.
42. CA TECHS., How To Survive and Thrive in the Application Economy 2 (2014).
43. See Zarate, supra note 1, at xiii (discussing the “centrality of American financial power and influence”).
times of distress.\footnote{ZARATE, supra note 1, at 9.} Eighty-one percent of the global trade financing is conducted using the American dollar.\footnote{BREMMER & KUPCHAN, supra note 1, at 9.} Because of its importance, our currency is the most counterfeited currency in the world by criminals and rogue states.\footnote{See FRANK W. ABAGNALE, THE ART OF THE STEAL 80 (2001) ("[T]he most counterfeited currency in the world is the American bill."); DICK K. NANTO, CONG. RESEARCH SERV., RL33324, NORTH KOREAN COUNTERFEITING OF U.S. CURRENCY 1 (2009).} Our markets in debt and equity securities dominate the global capital markets. Our institutions—both public and private—such as the Federal Reserve, the Securities and Exchange Commission (SEC), stock exchanges, and major investment banks are at the forefront of international financial policies and practices. As such, when America takes financial action, or when action is taken against American financial interests, it has global repercussions.\footnote{See ZARATE, supra note 1, at 12.} For example, following the September 11th attacks, financial rules and regulations promulgated by the United States against terrorism funding had a universal effect because of the unparalleled importance of the United States on the global financial system.\footnote{See Richard Barrett, Time To Reexamine Regulation Designed To Counter the Financing of Terrorism, 41 CASE W. RES. J. INT'L L. 7, 10–11 (2009).}

To be clear, while the financial infrastructure is American-centric, it is by no means completely controlled by the United States. America’s financial power is stymied in part by the rise of other geopolitical powers like the European Union and China. In fact, in 2015, China initiated the formation of the Asian Infrastructure Investment Bank with numerous international member states to serve as a financial counterweight to the United States.\footnote{See Jane Perlez, Rush To Join China’s New Asian Bank Surprises All, Even the Chinese, N.Y. TIMES, Apr. 3, 2015, at A5.} Additionally, a significant portion of America’s national debt is held by foreign nations, which has led national security experts like former Chairman of the Joint Chiefs of Staff, Admiral Mike Mullen, to remark, “[t]he most significant threat to our national security is our debt.”\footnote{ZARATE, supra note 1, at 413 (quoting Admiral Mike Mullen).} Similarly, in a high-tech financial framework, American financial institutions and businesses face global competition and challenges, as sovereignty matters less in the modern financial infrastructure.\footnote{See, e.g., Anne-Marie Slaughter, America’s Edge: Power in the Net-
Rogue regimes and bad actors could attempt to undermine the American financial dominance through new financial arrangements and the invention of new virtual payment systems.\textsuperscript{53} In sum, while the United States is the dominant force in the modern financial infrastructure, other nation-states and non-state actors will undoubtedly continue to challenge and compete with the United States for financial and economic power in the coming years.\textsuperscript{54}

B. \textsc{New Risks, Threats, and Vulnerabilities}

The modern financial infrastructure is both a valuable and vulnerable theater of war. Former Director of National Intelligence Michael McConnell estimated that a successful attack on a large American financial institution “would have an order-of-magnitude greater impact on the global economy’ than the Sept. 11, 2001, attacks.”\textsuperscript{55} This new financial theater of war presents new crosscutting risks, threats, and vulnerabilities. These new dangers can be broadly conceptualized as systemic and discrete perils, though this distinction is frequently obscured in many instances.

1. \textsc{Systemic Risks}

The modern financial infrastructure is subject to critical systemic risks and vulnerabilities due to its size, links, and speed.\textsuperscript{56} First, in terms of size, there exists the well-known systemic risk of “too big to fail,” which has garnered much atten-


\textsuperscript{54} See \textsc{Eric Schmidt & Jared Cohen, The New Digital Age: Transforming Nations, Businesses, and Our Lives} 82–89 (2014); Zarate, \textit{supra} note 1, at 385 (“Although the United States has had a near monopoly on the use of targeted financial pressure over the past ten years, this edge is likely to erode, leaving the United States both more vulnerable to external financial pressure and less able to use financial suasion as a lever of foreign policy.”); James D. Cox & Edward F. Greene, \textit{Financial Regulation in a Global Marketplace: Report of the Duke Global Capital Markets Roundtable}, 18 DUKE J. COMP. & INT’L L. 239, 239 (2007) (“U.S. capital markets face more competition than in the past.”).


\textsuperscript{56} See Scott, \textit{supra} note 6, at 673 (“Going forward, the central problem for financial regulation . . . is to reduce systemic risk.”).
tion in recent years.57 “Too big to fail” refers to the systemic risk where large financial firms become so integral to the stability of the economy that the state has to bail out these private firms with public funds when they are faltering.58 The existence of “too big to fail” firms presents large, important, and vulnerable targets in financial warfare. An attack on one or more of our large financial firms can cause significant damage to our national welfare. The Financial Stability Board has designated American financial firms like J.P. Morgan Chase, Citigroup, Goldman Sachs, Bank of America, Morgan Stanley, and Wells Fargo as Systemically Important Financial Institutions.59 In 2008, the failings of Bear Stearns and Lehman Brothers caused catastrophic economic stress at home and abroad.60 Had either of those firms failed because a foreign state or terrorist group attacked them, the economic and psychological damage would have been far more devastating.

Second, in terms of links, there exists the systemic risk of “too linked to fail.”61 Because of the interconnected and interdependent nature of the modern financial infrastructure, a disruption to certain firms and components that serve as important economic nodes in the system could lead to widespread


58. See, e.g., 12 C.F.R. § 1320.1(b) (2015); Amir E. Khandani et al., Systemic Risk and the Refinancing Ratchet Effect 48 (Harv. Bus. Sch., Working Paper No. 10-023, 2010) (“Systemic risk . . . arises when large financial losses affect important economic entities that are unprepared for and unable to withstand such losses, causing a cascade of failures and widespread loss of confidence.”).


60. See Bryan Burrough, Bringing down Bear Stearns, VANITY FAIR, Aug. 2008, at 106 (detailing how speculation about Bear Stearns liquidity problems turned into reality and caused Wall Street to falter); Carrick Mollenkamp et al., Lehman’s Demise Triggered Global Cash Crunch, WALL ST. J., Sept. 29, 2008, at A1; Andrew Ross Sorkin, Bids To Halt Financial Crisis Reshape Landscape of Wall St., N.Y. TIMES, Sept. 15, 2008, at A1 (stating Lehman Brothers would seek bankruptcy protection after failing to find a buyer).

61. See Lin, supra note 6, at 711–17.
damage and a significant blow to investor confidence. Distinct from the systemic risk of “too big to fail,” the systemic risk of “too linked to fail” includes smaller institutions and instruments whose distress or failure may ripple across the system because of their linkages, regardless of their value or size. For instance, in 1998, the Federal Reserve initiated a $3.6 billion private bailout for Long-Term Capital Management, a hedge fund with fewer than two hundred employees, because its demise would have generated significant losses for many investment banks and caused widespread panic in the international financial markets. Since then, hedge funds and other financial intermediaries have only grown larger in size, volume, and importance, further exacerbating the risks of “too linked to fail.”

In addition to hedge funds and other financial intermediaries, critical financial market components like clearinghouses, financial data farms, and securities information processors also present vulnerable targets in the financial theater of war because they serve as essential links in a multiplicity of financial networks. In 2015, the temporary failure of Bloomberg termi-

---

62. See PriceWaterhouseCoopers, What Investors Need To Know About Cybersecurity: How To Evaluate Investment Risks 1–5 (2014); Schmidt & Cohen, supra note 54, at 151–52; Schwarz, supra note 6, at 200; Waxman, supra note 5, at 424.

63. See Fin. Stability Bd., Assessment Methodologies for Identifying Non-Bank Non-Insurer Global Systemically Important Financial Institutions (2014); Schwarz, supra note 6, at 200 (discussing the systemic risks caused by financial intermediation and disintermediation); Shen Hong, Everbright Fiasco Casting a Shadow, WALL ST. J., Aug. 21, 2013, at C3 (reporting on the impact of a trading glitch at a medium-sized Chinese brokerage).


65. See Whitehead, supra note 6, at 5 (“Although hedge funds grew by 260% between 1999 and 2004 to become a one trillion dollar business, they were largely exempt from regulation under the federal securities and investment advisory laws.”).

66. See Henry T.C. Hu & Bernard Black, Debt, Equity and Hybrid Decoupling: Governance and Systemic Risk Implications, 14 EUR. FIN. MGMT. 663, 691 (2008) (“The longer the ownership chain . . . the greater the potential for agency costs and valuation errors to creep in.”); Judge, supra note 6, at 685; Yesha Yadav, The Problematic Case of Clearinghouses in Complex Markets, 101 GEO. L.J. 387, 389 (2013) (“Clearinghouses are stitched into the fabric of the financial markets and intrinsic to their operation.”); see also Steven L. Schwarz, Regulating Complexity in Financial Markets, 87 WASH. U. L. REV. 211, 215 (2009) (“Successful systems are those in which the consequences of a failure are limited. This can be done by decoupling systems through modu-
nals caused significant stresses in the global bond market affecting billions of dollars in transactions. Bloomberg, it should be noted, is not a large financial institution, but an information services provider with about 325,000 terminals used by financial traders. Yet, because of its important connective role in today’s financial network, its proper function is crucial to the system’s linked stability. The same is true for many of the other critical connective institutions of our financial system. For instance, an attack on the systems of the publicly obscure, but critically important, Depositary Trust & Clearing Corporation, which clears trillions of dollars in transactions daily, could cause significant economic and psychological damage to our national welfare. Lest one thinks that such attacks on our economic and financial infrastructure are farfetched and unlikely, two colonels of the Chinese People’s Liberation Army articulated using such attacks against the United States in a book about war strategy and tactics.

Third, in terms of speed, there exists the systemic risk of “too fast to save.” Transactions in the modern financial infrastructure occur at velocities measured in the milliseconds. Billions of dollars move through cables and spectra across seas and states in fractions of a second. While these astounding velocities can be beneficial in terms of efficiencies, they also in-

68. Id.
69. Id.
71. QIAO LIANG & WANG XIANGSUI, UNRESTRICTED WARFARE: CHINA’S MASTER PLAN TO DESTROY AMERICA 120–23 (2002).
72. See Lin, supra note 6, at 711–17.
73. See Fabozzi et al., supra note 39, at 8.
crease the risk of error, volatility, and market misconduct before anyone can intervene to prevent the damage.\textsuperscript{75} Further complicating the risks of “too fast to save” is the fact that many institutions engage in similar and interdependent strategies that are modeled on the same biases and assumptions.\textsuperscript{76} As a result, an attack on, or a failing of, one participant or one product could create vicious cycles of volatility for the entire financial infrastructure as actions cascade and generate feedback loops and spillover effects of serious systemic, adverse consequences.\textsuperscript{77} On May 6, 2010, the world witnessed an unprecedented stock market crash called the Flash Crash, which was allegedly caused by a single errant trade.\textsuperscript{78} In less than thirty minutes, approximately $1 trillion in market value vanished.


\textsuperscript{77} See Brown, supra note 33, at 7; Patterson, supra note 34, at 9–10 (discussing the financial dangers of “a vicious self-reinforcing feedback loop”); Louise Story & Graham Bowley, \textit{Market Swings Are Becoming New Standard}, N.Y. Times, Sept. 12, 2011, at A1.

from the U.S. stock market.\textsuperscript{79} While the Flash Crash was the result of an alleged programming error, it is not hard to imagine foreign states and terrorist organizations attempting to cause havoc on the homeland through similar attacks on our high-speed, automated financial systems. For instance, with the proliferation of automated trading platforms, cyber criminals can cause significant financial damage to the homeland from the comforts of a remote location and without firing a single shot simply by injecting bad data and false trades into the system.\textsuperscript{80}

2. Discrete Perils

Beyond the systemic perils, the new financial theater of war also presents a multitude of discrete perils. The modern financial infrastructure’s heavy reliance on computerized systems renders it particularly vulnerable to targeted cyberattacks.\textsuperscript{81} The Internet’s ubiquity means that any computer that is capable of being connected to the Internet is vulnerable to attack and malice.\textsuperscript{82} As the former Director of National Intelligence Mike McConnell observed: “[t]he United States is fighting a cyber-war today, and we are losing . . . . As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking.”\textsuperscript{83} Many serious crimes and attacks against American corporations now involve computers as the weapons of choice and cyberspace as the preferred setting.\textsuperscript{84} For many companies, software codes, intellectual property, and technological infrastructure represent some

\textsuperscript{79} Haldane, supra note 75, at 1.
\textsuperscript{80} See Michael Riley & Ashlee Vance, The Code War, BLOOMBERG BUSINESSWEEK, July 25, 2011, at 50.
\textsuperscript{81} See Hollis, supra note 7, at 1042 (speculating about computer viruses that incapacitate stock markets); Scott Patterson, CME Was the Victim of “Cyberintrusion” in July, WALL ST. J., Nov. 16, 2013, at B5; Riley & Vance, supra note 80, at 52.
\textsuperscript{82} See OFFICE OF THE NAT’L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, 2009–2011, at i (2011); Bambauer, supra note 7, at 1022 (“The Internet makes securing code much harder by exposing the inevitable bugs in software to sustained scrutiny and attack. Many—if not most—computers are connected to the Internet directly or indirectly.”).
\textsuperscript{83} Mike McConnell, To Win the Cyber-War, Look to the Cold War, WASH. POST, Feb. 28, 2010, at B1.
\textsuperscript{84} See BARRY VENGERIK ET AL., Hacking the Street? FIN4 Likely Playing the Market 3 (2014); Riley & Vance, supra note 80, at 52.
of the industry’s most valuable assets. General Keith Alexander, the former head of the National Security Agency and the U.S. Cyber Command in 2013, called the loss of American business secrets and intellectual property to cyber criminals “the greatest transfer of wealth in history.”

Enemies of the state can initiate numerous tactical cyber strikes on American interests in the financial theater of war causing serious harms and significant damage. This was made alarmingly real by the 2014 hack of Sony Pictures, an American subsidiary of Sony Corporation, by North Korea. A number of similar cyberattacks have been made on American banks and other financial institutions by foreign states and rogue organizations. While the full measure of the costs resulting from such attacks is frequently hard to quantify, these costs are nonetheless real and potentially enormous, particularly the intangible and psychological damages that fall out from these attacks. Due to the amorphous and anonymous nature of cyberattacks—and the reticence of corporate victims to come forward—attrition, prevention, prosecution, and counterstriking can all prove to be difficult.

85. See Brown, supra note 33, at 49 (discussing the urgent need for blackbox firms to safeguard successful strategies for as long as possible); David Barboza & Kevin Drew, Security Firm Sees Global Cyberspying, N.Y. TIMES, Aug. 4, 2011, at A11 (“Cybersecurity is now a major international concern, with hackers gaining access to sensitive corporate and military secrets, including intellectual property.”); Alex Berenson, Arrest over Trading Software Illuminates a Secret of Wall St., N.Y. TIMES, Aug. 24, 2009, at A1 (noting the importance of computer programs to financial institutions).

86. Seabrook, supra note 13 (quoting General Keith Alexander).

87. See Brown, supra note 5, at 182; Sean S. Costigan, Terrorists and the Internet: Crashing or Cashing in?, in TERRORNOMICS 113, 117 (Sean S. Costigan & David Gold eds., 2007) (noting the FBI estimated that cybercrime costs the U.S. $400 billion annually); Kelsey, supra note 5, at 1434 (“If properly executed, the result of the cyber strike would be the same as a conventional bombing raid but without the risk of civilian or military causalities.”); Seabrook, supra note 13, at 65 (“A large part of the nation’s financial infrastructure is under siege [from cyberattacks].”).


89. See infra notes 96–103.


91. See, e.g., Mark Bowden, WORM: THE FIRST DIGITAL WORLD WAR 48–
Outside of the risks based in cyberspace, globalization has also created more discrete vulnerabilities for American financial interests. Major American corporations have significant international footprints that can subject them to foreign economic pressures and threats. For instance, Caterpillar, the multi-billion dollar manufacturer of heavy machinery based in Peoria, Illinois, has operations in six continents, subjecting them to serious financial risks from foreign governments and non-state actors abroad.\footnote{See Caterpillar, Inc., Annual Report (Form 10-K), at 9–11 (Feb. 18, 2014).} Similarly, Goldman Sachs, a New York-based investment bank, has offices in over thirty countries with fifty percent of their headcount and forty-two percent of their revenues coming from outside of North America and South America.\footnote{See The Goldman Sachs Grp., Inc., Annual Report (Form 10-K), at 1 (Feb. 28, 2014).} Every international office or facility of an American corporation like Goldman Sachs and Caterpillar can represent a valuable target for our enemies in financial warfare, and an attack on a significant foreign office or facility of a major corporation can cause significant economic and psychological harm to American interests.

C. NEW AND OLD ADVERSARIES

The financial theater of war presents a diverse lineup of new and old adversaries relative to adversaries of traditional theaters of war. In traditional warfare, nation-states with uniformed soldiers were the clear, predominant adversaries. In the financial theater of war, adversaries are less clear and more diverse. In modern financial warfare, antagonists include famil-
iar foes like nation-states, but they also include less familiar foes like terrorist organizations, lone-wolf hackers, rogue employees, foreign corporations, domestic criminals, anarchists, and a host of cyber bad actors.94 Further complicating matters is the fact that a technologically interconnected world has led to the rise of cyber mercenaries willing to cause harm and havoc for the right price.

Episodes from recent history reveal the diversity of potential adversaries engaging in financial warfare. In 2011, hackers threatened Bank of America with stolen, corporate information.96 In 2012, large, coordinated attacks, some attributable to Iran, dubbed “Operation High Roller,” targeted American and international financial institutions.97 In 2013, hackers infiltrated the Associated Press’s Twitter account to falsely broadcast an attack on the White House that temporarily erased $136 billion in market value when automated programs traded on the bogus news.98 In 2014, it was revealed that Russian


95. See HARRIS, supra note 7, at 103–22 (discussing the market for cyber mercenaries); Matthew Goldstein, Need Some Espionage Done? Hackers Are for Hire Online, N.Y. TIMES, Jan. 16, 2015, at A1.


hackers infiltrated the NASDAQ computer system, and they continue to develop a sophisticated arsenal of cyber weapons to use against other nation-states. That same year, a group of cyber criminals dubbed as FIN4 hacked into the computer systems of Wall Street firms and other American corporations with the goal of stealing information that could affect the global financial markets. In 2015, it was revealed that an international cyber gang systemically stole millions of dollars from over one hundred institutions around the world. Later that year, an international syndicate of traders and hackers were charged with operating a massive insider trading enterprise. Furthermore, in recent years, China has been privately suspected and publicly accused of serious cybercrimes against American interests. In fact, the United States took the extraordinary step of indicting five Chinese military officials in 2014 for hacking into U.S. corporations to commit espionage and intellectual property theft.

In addition to an expanding cast of external adversaries, financial institutions must also guard against potential internal adversaries. Rogue employees or contractors with author-


105. See Bambauer, supra note 7, at 1050 ("[I]t is not technologically possi-
ization and access can cause some of the most devastating damage to a country, its national security, and its financial interests. Robert Hanssen, who spied for the Soviet Union and Russia for over twenty years, and caused the most destructive breach in domestic intelligence, was an FBI agent. Edward Snowden, who initiated one of the largest leaks of classified documents and defense programs in history in 2013, was a National Security Agency (NSA) contractor. Similarly, a rogue programmer or banker with access to critical infrastructure or operational software can cause havoc for the financial system. In 2015, it was revealed that a Morgan Stanley financial advisor allegedly stole over 300,000 confidential client account records, and that information was later placed online for sale.

In sum, a diverse and expanding cast of familiar and unfamiliar foes in financial warfare makes this new theater of war one of the most challenging terrains for present and future battles.

*   *   *

Finance is the lifeblood of the American economy. Strong and stable financial institutions make for a stronger America. During the recent financial crisis when American investment banks were in distress, the entire economy and country suffered. Venerable American corporations like General Electric had difficulties funding day-to-day operations. McDonald’s

---


109. See Dune Lawrence, Tracking the Enemy Within, BLOOMBERG BUSINESSWEEK, Mar. 16, 2015, at 39 (reporting on the “insider threat” relating to cybersecurity from employees); see also MARK RUSSINOVICH, ROGUE CODE (2014) (depicting a fictional account of a rogue programmer causing global financial panic).


112. See SORKIN, supra note 57, at 417.
franchisees struggled to get loans to make payroll.\textsuperscript{113} General Motors went into bankruptcy.\textsuperscript{114} And millions of Americans lost their homes, their jobs, and their peace of mind.\textsuperscript{115} Given the importance of finance to America and the intertwined nature of modern economies, it should be little wonder that the new theater of war is the modern financial infrastructure, a place filled with new risks, threats, and vulnerabilities targeted by a cast of familiar and unfamiliar foes.

II. FINANCIAL WEAPONS OF WAR

The armaments of modern financial warfare are as vast, diverse, and important as the myriad of ways to raise and move money.\textsuperscript{116} Broadly, the financial weapons of war can be divided into analog weapons and cyber weapons, both of which can be used for offensive and defensive purposes. Analog weapons include policy actions, such as economic sanctions, anti-money laundering regulations, and banking restrictions. Cyber weapons include distributed denial-of-service attacks, data manipulation hacks, and destructive intrusions. Modern financial warfare often involves the concerted use of both analog and cyber financial weapons of war.

A. ANALOG WEAPONS

Analog financial weapons have long been used in connection with warfare to cut off funding for adversaries.\textsuperscript{117} Ancient Greek and Roman empires deployed financial and economic tactics to decimate their adversaries.\textsuperscript{118} As a young nation, the

\textsuperscript{113} Id.
\textsuperscript{114} See ALEX TAYLOR III, SIXTY TO ZERO: AN INSIDE LOOK AT THE COLLAPSE OF GENERAL MOTORS—AND THE DETROIT AUTO INDUSTRY 1 (2010).
\textsuperscript{115} See Alicia Parlapiano et al., The Nation’s Economy, This Side of the Recession, N.Y. TIMES (June 14, 2014), http://www.nytimes.com/interactive/2014/06/14/business/this-side-of-the-recession.html.
\textsuperscript{116} See U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-04-163, TERRORIST FINANCING: U.S. AGENCIES SHOULD SYSTEMATICALLY ASSESS TERRORISTS’ USE OF ALTERNATIVE FINANCING MECHANISMS 9–22 (2003) (describing various methods terrorist organizations use to raise money); ZARATE, supra note 1, at 384 (“The conflicts of this age are likely to be fought with markets, not just militaries, and in boardrooms, not just battlefields. Geopolitics is now a game best played with financial and commercial weapons.”).
\textsuperscript{117} See GARY CLYDE HUFBAUER ET AL., ECONOMIC SANCTIONS RECONSIDERED 9–17 (2009) (providing a historical overview of economic sanctions).
\textsuperscript{118} See KERN ALEXANDER, ECONOMIC SANCTIONS: LAW & PUBLIC POLICY 8 (2009) (“Indeed, Athens imposed economic sanctions in 432 BC when Pericles issued the Megarian import embargo against the Greek city-states which
United States imposed the Embargo Act of 1807 to maintain its neutrality in the war between Britain and France, as well as to punish the British.\(^{119}\) Later in the twentieth century, during the Cold War, the United States imposed a series of economic sanctions against the Soviet Union and its Communist allies.\(^{120}\) In the days following the September 11th attack on the United States, the United Nations Security Council unanimously adopted Resolution 1373 applicable to all member states, which required compliance with its International Convention for the Suppression of the Financing of Terrorism.\(^{121}\) Additionally, the G7 nations, through their Financial Action Task Force, also adopted several recommendations against terrorist financing following September 11, 2001.\(^{122}\) Notwithstanding these efforts, terrorist organizations and rogue nations continue to use duplicitous and clandestine means to gain access to funding in the global financial system.\(^{123}\) As a result, at the beginning of the twenty-first century, despite all the technological advances in finance, analog financial weapons continue to play an im-

---

important role in the financial theater of war. Chinese military officials have openly discussed using financial warfare in international conflicts. The United States, as the lone financial superpower in the world, has creatively and effectively used many analog financial weapons against its adversaries. In the years following September 11th, the United States has made concerted efforts to choke off funding for terrorist organizations like al Qaeda and ISIS. Similarly, it has used denial of access to the global financial system and economic sanctions to respond to aggression by North Korea, Syria, Iran, and Russia. Three general crosscutting categories of such analog weapons are worth noting: economic sanctions, anti-money laundering regulations, and banking restrictions.

First, in terms of economic sanctions, nation-states have long used such policy tools as part of warfare and conflict, and they have become more prevalent in recent years. Economic sanctions are designed and intended to cause financial damage and distress to an enemy in a hot war or a cold war. Economic sanctions can be targeted against nation-states or specific individuals and institutions. The United States has had sanctions against North Korea since the Korean War in the 1950s. Economic sanctions can include policies like asset freezes, import tariffs, trade barriers, travel restrictions, and embargoes.

124. See QIAO & WANG, supra note 71, 39–41.
125. See ZARATE, supra note 1, at ix (“Far from relying solely on the classic sanctions or trade embargoes of old, these [financial pressure] campaigns have consisted of a novel set of financial strategies that harness the international financial and commercial systems to ostracize rogue actors and constrict their funding flows, inflicting real pain.”).
126. Id. at v–ix.
127. Id.
129. See BRENDAN TAYLOR, SANCTIONS AS GRAND STRATEGY 31 (2010).
China has used embargoes of rare earth minerals, which are predominantly mined in China and crucial to electronics, to exert pressure on Europe, Japan, and the United States. More recently, the Treasury Department’s Office of Foreign Assets Control (OFAC) has overseen a host of longstanding and new financial sanctions as a tool in modern warfare against American adversaries as varied as the Iranian Revolutionary Guard, terrorist organizations, Mexican drug traffickers, and foreign nation-states. For instance, in 2014, the United States and its allies imposed a series of crippling economic sanctions against Russia and several Russian citizens following Russia’s annexation of Crimea. More recently, in 2015, due partially to economic sanctions, Iran and the key stakeholders in the international community reached a historic agreement that attempts to limit its nuclear weapons program.

Second, in terms of anti-money laundering regulations, nation-states have been more aggressive and expansive in using such regulations to prevent the flow of ill-gotten gains and legitimate capital towards funding terrorist and enemy war efforts. Anti-money laundering regulations have placed financial institutions at the frontlines of financial warfare. Financial institutions are now required to identify their customers and report suspicious financial transactions to govern-

(2009) (describing restrictive designations and asset freezes in connection with terrorist financing); Lowrey, supra note 15.
135. See, e.g., U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing—HSBC Case History: Hearing Before the Permanent Subcomm. on Investigations of the S. Comm. on Homeland Sec. & Gov’t Affairs, 112th Cong. 10–12 (2012) (statement of David S. Cohen, Undersecretary for Terrorism and Fin. Intelligence, Dep’t of the Treasury); Baradaran et al., supra note 1, at 488–90 (describing anti-money laundering efforts initiated by the United States); Richard K. Gordon, Losing the War Against Dirty Money: Rethinking Global Standards on Preventing Money Laundering and Terrorism Financing, 21 DUKE J. COMP. & INT’L L. 503, 505 (2011) (“Over the past forty years anti-money laundering rules have been expanded . . . .”).
ment authorities or they could be subject to criminal prosecution.\textsuperscript{137} Following the September 11, 2001 attack on the United States, the USA PATRIOT Act was passed. Title III of the Act focused on money laundering and terrorism financing.\textsuperscript{138} Additionally, post-September 11th, many nations joined forces to help prevent the flow of funds to al Qaeda through new anti-money laundering regulations.\textsuperscript{139} For instance, the Group of Ten countries that manage the Society for Worldwide Interbank Financial Telecommunications (SWIFT), which is used for a significant percentage of global financial transactions, gave the United States access to its database to track and trace illicit flows of funds to terrorists and rogue nations.\textsuperscript{140} Documents found in Osama Bin Laden’s compound revealed that the global efforts to restrict terrorist funding had made it frustratingly more difficult for al Qaeda to raise and transfer money around the world.\textsuperscript{141} In current global conflicts with Russia, Syria, Iran, and North Korea, the United States and its allies continue to impose and enforce strict anti-money laundering regulations as a tactic against its adversaries.\textsuperscript{142} Furthermore, in the current battle against ISIS, one of the most well-funded terrorist organizations in history, the Treasury Department’s anti-money laundering efforts, in particular efforts through its Office of the Comptroller of the Currency, are on the frontlines of this battle.\textsuperscript{143} ISIS has been estimated to possess in excess of $500 million in assets through ransoms, looting, extortion, and the capacity to generate $500 million from oil revenue annually to fund its reign of terror.\textsuperscript{144} Because money is so critical to its

\textsuperscript{137} See id.; Ben Protess & Jessica Silver-Greenberg, Bank Said To Avoid Charges over Laundering, N.Y. TIMES, Dec. 11, 2012, at A1 (reporting on the record $1.92 billion fine levied against HSBC for failing to comply with anti-money laundering regulations).
\textsuperscript{139} See International Convention for the Suppression of the Financing of Terrorism, supra note 121; S.C. Res. 1373, supra note 121.
\textsuperscript{140} See ZARATE, supra note 1, at 49–59.
\textsuperscript{141} Id. at ix.
\textsuperscript{142} Lowrey, supra note 15.
\textsuperscript{144} See Donna Abu-Nasr & Larry Liebert, It’s More Than Just Oil, BLOOMBERG BUSINESSWEEK., Nov. 23, 2015, at 11–12; Matthew Rosenberg et al., How ISIS Wrings Cash from Those It Now Controls, N.Y. TIMES, Nov. 30,
reign of terror, these anti-money laundering regulatory weapons designed to cut off its funding are just as important in this battle as traditional weapons of bullets and bombs.

Third, in terms of banking restrictions, nation-states utilize designations and bans to prevent their adversaries from fully accessing the global banking system. Because of the interconnectedness of modern finance, and the central role of the United States in it, such restrictions can render a nation-state or organization isolated from the global financial system and unable to secure financing for its war efforts and rogue operations since legitimate institutions fear the reputational risks of being associated with rogue organizations. In a financial system that revolves around the United States, American financial weaponry is far-reaching and can enlist foreign financial institutions for assistance. For example, as part of the war against terrorism, the United States designated certain charities and organizations as “terrorist organizations,” and denied them access to the global financial system since any institution conducting business with a designated organization would be prohibited from engaging in financial dealings with any American entity, corporation, or individual. Additionally, because the U.S. dollar serves as the reserve currency of the world, banking restrictions have the practical effect of making it extremely difficult for a restricted party to conduct any meaningful transactions around the world. In 2014, the United States imposed a series of sanctions against firms and individuals close to Russian President Vladimir Putin that essentially froze those “individuals and institutions out of the vast swath of the global financial market denominated in dollars.”

---


146. See ZARATE, supra note 1, at 349 (“The reality was that in the new age of financial pressure and a global financial system, American demands and practices applied globally.”).


149. Lowrey, supra note 15, at B5.
ly, American regulators fined Commerzbank, a German financial corporation, almost $1.5 billion for providing banking services for certain designated Iranian businesses. In sum, given the importance of the United States in the global financial system, banking restrictions and designations could choke off access to any legitimate financial infrastructure for an adversary and render them an outcast to much of the international financial community.

While no weapon and no defense can perfectly prevent every attack from an adversary, thoughtful targeted strikes using analog financial weapons can seriously blunt the efforts of our enemies. In recognition of the importance of the analog financial weapons of war, the United States has invested substantial resources in building up its capabilities. The Treasury Department now has its own intelligence and counterterrorist unit consisting of over 700 individuals with an annual budget of $200 million to fight a diverse and expanding cast of adversaries using various analog weapons of war.

B. Cyber Weapons

As with the emergence of analog financial weapons, cyber financial weapons have also emerged as critical armaments in modern warfare with the rise and proliferation of the Internet and information technology. America’s heavy financial and military reliance on high-tech informational networks render it particularly vulnerable to cyber weapons. The volume and...
varieties of cyberattacks on financial institutions, like all cyberattacks, increase annually. In modern financial warfare, the first shots of the battle are frequently fired in cyberspace. As an early example, in 2007, during a dispute with Russia, the Baltic nation-state of Estonia experienced a massive cyberattack on its entire cyber infrastructure, which partially paralyzed the country’s banking system and entire online infrastructure. Disclosures by Edward Snowden of classified documents indicated that the United States had initiated over 200 offensive cyberattacks in 2011 against China, Iran, Russia, and North Korea, many with important military and economic implications. More recently, in 2014, around the time of the Ukrainian presidential elections, it has been reported that Russia unleashed a series of cyberattacks on the election commission, military forces, and other governmental entities of Ukraine.

The truth of the matter is that cyber weapons of financial war and cyber weapons in general have become more varied, more sophisticated, and more prevalent in modern warfare. In 2013, General Keith Alexander, the then head of U.S. Cyber Command, announced that the Pentagon would have thirteen offensive cyber teams by 2015. A 2015 Pentagon report found “significant vulnerabilities on nearly every” weapons program under its control. A 2015 Wall Street Journal study reported

destructive cyberattack could present a significant risk to U.S. economic and national security if lives are lost, property destroyed, policy objectives harmed, or economic interests affected.”; Waxman, supra note 5, at 424 (“[E]lectronic and informational interconnectivity creates tremendous vulnerabilities, and some experts speculate that the United States may be especially at risk because of its high economic and military dependency on networked information technology.”).

156. See FIN. INDUS. REGULATORY AUTH., REPORT ON CYBERSECURITY PRACTICES 1 (2015).


161. DEPT’F OF DEF. OFFICE OF THE DIRECTOR, OPERATIONAL TEST AND
“29 countries now have formal military or intelligence units dedicated to offensive cyberefforts.” A recent survey of American financial institutions indicated that attacks from other nation-states and hackers using cyber weapons are some of their most pressing concerns. In 2013 alone, it has been reported that “the average American company fielded a total of 16,856 attacks” from cyber weapons. In response to the rise of cyber weapons, in 2015 President Obama issued an executive order that empowered the Treasury Secretary to block the financial assets of individuals that use cyber weapons to harm the national security and economic welfare of the United States. Three broad, interrelated categories of such weapons are worth highlighting in connection with financial cyberwarfare: distributed denials-of-services attacks, data manipulation hacks, and destructive intrusions.

First, distributed denials-of-services (DDoS) attacks are cyber incursions that attempt to disrupt and suspend the service of an online host to its users, and are one of the most common forms of cyberattacks. DDoS attacks frequently operate by flooding a site with illegitimate traffic and requests until that site is overwhelmed and all services are suspended. In 2008, Russia concurrently launched a cyberwar in addition to a traditional war against Georgia by deploying a series of DDoS attacks against key Georgian computer systems. In 2012, six major American banks were subjected to DDoS attacks by an organization called the Izz ad-Din al-Qassam Cyber Fighters that rendered their online services temporarily inaccessible to their customers and clients. A year later, major banks were again subjected to another round of persistent DDoS attacks,

---

166. See Hathaway et al., supra note 5, at 837.
168. See, e.g., Perlroth, supra note 97.
but this time from the nation-state of Iran.\footnote{169} In 2015, it was reported that China possessed a cyber weapon that could intercept and re-direct a tsunami of Internet traffic to sites that it wanted to shut down.\footnote{170} To date, DDoS attacks on our financial institutions have all been temporary in their effects, but they could cause serious and lasting damage. For instance, a successful DDoS attack on the New York Stock Exchange or the NASDAQ during a normal trading day could cause massive financial chaos and possibly an economic crisis, to say nothing of the psychological and emotional toll on American and international citizens.

Second, data manipulation hacks, or semantic attacks, can serve as another powerful cyber weapon of financial warfare. Data manipulation hacks or semantic attacks describe cyber aggressions that are intended to plunder or maliciously alter data towards destructive ends.\footnote{171} Enemies of a state can hack their way into the networks of financial institutions and steal or manipulate critical data that then could be used to cause economic chaos on a country and possibly the entire global financial system. Industry-wide studies about cybersecurity conducted in 2011 and 2014 indicated that financial firms were most concerned with data manipulation hacks.\footnote{172} Events in recent years give those firms good cause for concern. In 2014, it was reported that Iran initiated a series of coordinated cyberattacks in sixteen countries with the goal of stealing and manipulating data related to critical infrastructure and financial operations.\footnote{173} That same year, hackers attacked J.P. Morgan Chase and stole gigabytes of data that gave them access to numerous customer accounts and millions of dollars in funds.\footnote{174} While much of the damage arising from data manipulation attacks has been limited, a far more damaging attack is foreseeable. The late popular novelist, Tom Clancy, described a night-

169. See, e.g., Perlroth & Hardy, supra note 97.
172. FIN. INDUS. REGULATORY AUTH., supra note 156, at 4.
mare scenario in his novel *Debt of Honor*, in which enemies of the state maliciously injected falsified data into the American securities markets causing global financial chaos as automated programs instantaneously reacted to the bad information before it could be detected.\textsuperscript{175}

Third, in addition to DDoS attacks and data manipulation hacks, destructive intrusion attacks are cyber weapons that are used to destroy critical financial infrastructure.\textsuperscript{176} The antagonists would deploy such cyber weapons against a critical financial target with the goal of destroying the target rather than disrupting it. During the lead up to the Iraq War in 2003, the United States considered launching a cyberattack to destroy the Iraqi financial system prior to commencing bombing but ultimately declined to do so for fear of creating financial chaos in the region.\textsuperscript{177} Similarly, a terrorist organization can attempt to destroy the New York Mercantile Exchange by using a computer virus to attack the servers of the exchange in a manner that would lead to systemic failures and chaos in the commodities market. It has been alleged that, in 2011, the United States and Israel unleashed Stuxnet, a computer virus superworm, deemed by some at the time as “the most sophisticated cyber weapon ever deployed,” to destroy an Iranian nuclear weapons facility.\textsuperscript{178} Stuxnet destroyed the centrifuges in the nuclear facility by clandestinely reprogramming them to overwork until destruction.\textsuperscript{179} A year later, it was reported that another computer super virus called the Flame—which some again attributed to the United States and Israel—was “afflicting computers in Iran and the Middle East.”\textsuperscript{180}

\begin{flushright}
175. See Tom Clancy, *Debt of Honor* 294–312 (1994). While this scenario may appear far-fetched, in the same novel Mr. Clancy also envisioned enemies of America intentionally crashing jets into strategically important buildings, which became a reality on September 11, 2001. See id. at 760–64.


177. See Zarate, supra note 1, at 170 (“[P]lanners had devised strategies for a possible cyberattack to disrupt the financial structure of the Iraqi state.”).


179. Broad et al., supra note 178.

\end{flushright}
it was reported that the United States has embedded “surveillance and sabotage tools” in targeted computer systems of its adversaries in Iran, Russia, Pakistan, China, Afghanistan, and other countries. In 2015, it was also reported that Russian hackers had breached Pentagon and White House computer systems, including some of President Obama’s emails. That same year, it was alleged that China hacked into the computer systems of the Office of Personnel Management and acquired the private information of over 21.5 million people with ties to the federal government, which amounted to “apparently the largest cyberattack into the systems of the United States government.”

While a major destructive cyberattack has yet to occur in the homeland to our financial infrastructure or other critical infrastructure, our adversaries are likely planning such attacks. Former U.S. Secretary of Defense Leon Panetta warned a few years ago that the United States was facing a potential “cyber–Pearl Harbor” in the near future.

Cyberattacks can be particularly challenging to defend against, although public and private actors have made significant strides in improving cybersecurity in recent years. Recognizing the seriousness of cyber weapons against the financial system and other American interests, the federal government has responded to this emerging threat with more aggressive and strategic cyber-defense and cyber weapons programs in re-

183. Davis, supra note 103.
186. See, e.g., Bowden, supra note 91 (describing challenges in creating a cybersecurity defense system); Gordon & Ford, supra note 91 (“Despite the fact that the word ‘Cybercrime’ has entered into common usage, many people would find it hard to define the term precisely.”); Hathaway et al., supra note 5, at 874–77 (opining on legal challenges to addressing cyberattacks); Roberts, supra note 91 (acknowledging difficulties in tracing the origins of cyberattacks); Gross, supra note 91, at 220 (“Because virtual attacks can be routed through computer servers anywhere in the world, it is almost impossible to attribute any hack with total certainty.”); Matthews, supra note 91; Strohm et al., supra note 91 (reporting on the reluctance of companies to disclose cyber attacks).
187. See Costigan, supra note 87, at 117 (noting the FBI estimated that cybercrime costs the U.S. $400 billion annually).
cent years. In 2012 alone, the Air Force spent about $4 billion on its cyber programs, and the Labor Department, in response to cyber threats, improved the computer security of its valuable economic data. In 2013, it was revealed that President Obama possessed broad powers relating to cyberstrikes against our enemies. That same year, President Obama also issued an executive order aimed at enhancing cybersecurity, and established the U.S. National Institute for Standards and Technology Cybersecurity Framework to encourage the public-private information sharing on best cybersecurity practices. In 2015, the White House announced a new executive order on cybersecurity and the creation of the Cyber Threat Intelligence Integration Center under the Office of the Director of National Intelligence to better monitor and respond to cyberthreats; and the Cybersecurity Act of 2015 was signed into law as part of an omnibus spending bill. That same year, the Department of Defense also released a comprehensive white paper on its cyber strategy. In 2016, the White House announced a Cybersecurity National Action Plan intended to initiate near term and long term actions towards enhancing cybersecurity. In addition to the panoply of government action, private firms have also made greater efforts to secure their information sys-

188. See, e.g., DEP’T OF DEF., CYBERSPACE POLICY REPORT (2011); DIV. OF CORP. FIN., SEC. & EXCH. COMM’N, DISCLOSURE GUIDANCE: TOPIC NO. 2: CYBERSECURITY (2011); WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD (2011); James Bamford, The Silent War, WIRED, July 2013, at 90.

189. See Julian E. Barnes, Pentagon Digs in on Cyberwar Front, WALL ST. J., July 6, 2012, at A4 (stating that “overall the Air Force spends about $4 billion a year on its cyber programs”).


194. DEP’T OF DEF., supra note 94.

tems and purchase insurance in connection with these attacks. Despite all these efforts, as financial warfare grows and evolves, perfect cybersecurity is impossible in an interconnected world, so industry and government sentinels must remain vigilant of the growing and evolving threats.

III. OLD RULES AND NEW CONCERNS

War poses problems for law. Cicero, the Roman philosopher and politician, bleakly stated that, “In time of war, law is silent.” New concerns raised by the brutality and unpredictability of war, at times, render law unfit to address many of them. Emerging financial warfare is no different. The policy challenges posed by financial warfare are rooted deeply in core tensions between the conventional laws of war and the realities of the world. War and peace today look very different than in eras past. In fact, the differences between war time and peace time have become less distinct. As such, many of the old rules, old modes, and old ways of the past are not suitable for addressing some of the challenges of the present and the emerging future of conflict and war. Questions and issues about how longstanding laws and norms about war should govern financial hostilities, cyberattacks, and non-state actors are at the heart of these core tensions.

A. OF FINANCIAL HOSTILITIES

The laws and norms of war—the *jus ad bellum* and *jus in bello* principles—have long defined triggering events for war and wartime conduct primarily in the context of armed conflicts between and among nations. For instance, the North Atlantic

196. See Perlroth & Harris, supra note 90.
197. See Bambauer, supra note 7, at 1017 (“[T]here is a nascent realization that . . . it is impossible to completely solve cybersecurity problems . . . .”).
199. See DAVID KENNEDY, OF WAR AND LAW 3 (2006) (“War and peace are far more continuous with one another than our rhetorical habits of distinction and our wish that war be truly something different would suggest.”).
201. See, e.g., Todd C. Huntley & Andrew D. Levitz, Controlling the Use of Power in the Shadows: Challenges in the Application of Jus in Bello to Clandestine and Unconventional Warfare Activities, 5 HARV. NAT’L SEC. J. 461,
Treaty Organization (NATO) in Article 5 of its founding Washington Treaty of 1949 states that “an armed attack against one [member state] or more of them in Europe or North America shall be considered an attack against them all.” Yet no clear laws or widely accepted norms govern attacks that are economic and financial in nature where traditional arms are not used, even though the damage can nonetheless be just as devastating.

Part of the tension that arises from attempting to apply traditional laws and rules of war from the context of warring nation-states to economic and financial hostilities is rooted in the view that such hostilities are better understood in the context of commerce, crime, and diplomacy, not warfare. This perspective is supported by a longstanding understanding that economic coercion is generally not considered a prohibited use of force for purposes of international law. In fact, drafters of the United Nations Charter considered and rejected the view that economic coercion should be a prohibited use of force. The United Nations, furthermore, has long used economic sanctions as one of its governance tools. Additionally, states regu-
larly and lawfully use economic coercion in dealing with their adversaries, thereby giving more credence to the view that economically coercive policies are not prohibited uses of force. While this perspective is correct in many instances, it is not correct in all instances. A severe, unprovoked tariff on American imports by a foreign state should not be considered an act of economic or financial hostility in the context of warfare. Alternatively, a severe, unprovoked attempt to destroy the proper functions of the New York Stock Exchange with the intent of harming the American financial system by a foreign state should warrant closer consideration as an act of war. These two scenarios present easier cases. The more vexing cases arise when the lines demarcating the spheres of commerce, crime, diplomacy, and warfare blur and intersect.

Direct actions against American economic and financial interests in recent years by our adversaries have further obscured the distinctions among commerce, crime, diplomacy, and warfare. Additionally, these attacks frequently do not distinguish between civilians and non-civilians. When a financial institution is attacked, both civilians and non-civilians may be harmed. China has been suspected of concerted state-sponsored cyberattacks and espionage against private American financial institutions for many years. The Russians have hacked into the NASDAQ, and have made covert attempts to destabilize our capital markets. Iran has made sustained effort to desta-

208. See Gervais, supra note 205 (“In practice, economic coercion is an accepted tactic in international relations. States regularly use loans, credits, and foreign aid, among other means, to influence state action in designed ways.”).

209. See Tom J. Farer, Political and Economic Coercion in Contemporary International Law, 79 AM. J. INT’L L. 405, 408–09 (1985); John Richardson, Stuxnet As Cyberwarfare: Applying the Law of War to the Virtual Battlefield, 29 J. MARSHALL J. COMPUTER & INFO. L. 1, 11 (2011) (“Damage to these institutions . . . while not damaging physical infrastructure can have a far greater impact on a state’s economy.”); Waxman, supra note 5, at 424–30.

210. See Eric Talbot Jensen, Cyber Warfare and Precautions Against the Effects of Attacks, 88 TEX. L. REV. 1533, 134–36 (2010); Sales, supra note 7, at 1524.

211. See, e.g., Ariana Eunjung Cha & Ellen Nakashima, Google Attack Part of Vast Campaign; Targets Are of Strategic Importance to China, Where Scheme Is Thought To Originate, WASH. POST, Jan. 14, 2010, at A1; Dune Lawrence & Michael Riley, A Portrait of a Chinese Hacker, BLOOMBERG BUSINESSWEEK, Feb. 18, 2013, at 54; Sanger et al., supra note 103; Sanger & Landler, supra note 103.

212. See Riley, supra note 99; Benjamin Weiser, 3 Men Are Charged with Serving as Secret Agents for Russia in New York, N.Y. TIMES, Jan. 27, 2015, at A16.
bilize our banking system through persistent cyberattacks. Various non-state actors have also made serious attempts to cause significant damage to our civilian financial institutions.

As cool and cold wars grow warm and hot, these tensions between traditional laws of war and modern financial hostilities will continue to persist. Therefore, American and international policymakers need to take a more proactive approach with the governance of financial weapons in modern conflicts by resolving the existing tensions of traditional laws of warfare and contemporary realities. If a complete resolution of these tensions is not possible in the near future, policymakers should, at minimum, articulate a set of clear guiding principles for the road ahead.

B. OF CYBERATTACKS

The traditional laws and norms of war and armed conflict are not well suited to address many of the new concerns relating to attacks based in cyberspace. There are no clear strategies for cyberattacks despite the enormous potential financial fallout and physical destruction that can occur from cyberattacks. Numerous basic questions about cyberattacks in the financial realm and beyond continue to lack a wide and

213. See, e.g., Perlroth & Hardy, supra note 97.
214. See, e.g., Schwartz, supra note 96.
216. See Waxman, supra note 5, at 435 (suggesting a more expansive legal view of wartime hostilities that includes harms like “a take-down of banking systems, causing cascades of financial panic”).
217. See Brown, supra note 5, at 180–82; Hathaway et al., supra note 5, at 840 (“Applying the existing law of war framework to cyber-attacks is extraordinarily challenging.”); Hollis, supra note 7, at 1023 (discussing how states must wrestle with the emerging issues relating to information operations in cyberspace); Larry May, The Nature of War and the Idea of “Cyberwar,” in CYBERWAR, supra note 7, at 6–15 (expounding on the differences between traditional wars and cyberwars).
clear consensus among key international stakeholders.\textsuperscript{219} These basic questions are rooted partially in fundamental issues relating to sovereignty, weaponry, and governance.

First, in terms of sovereignty, cyberattacks raise pressing issues about jurisdiction.\textsuperscript{220} As a general matter of international law, a sovereign’s legal powers normally end at its borders, but warfare in cyberspace pays little regard to national boundaries.\textsuperscript{221} Is cyberspace a new extra-sovereign domain given its inherent extra-territorial nature?\textsuperscript{222} Scholars and policymakers have wrestled with this question since the early days of the Internet, and this question has serious implications for laws of war.\textsuperscript{223} The United States has defined cyberspace as “the inter-
dependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. The United States and a few other countries including China, Iran, Israel, and the United Kingdom have referred to cyberspace as a domain for military purposes. Nonetheless, unlike traditional warfare, there remains no clear consensus on this important question relating to sovereignty and jurisdiction. Traditional wars and armed conflicts take place with more understood weapons and within less disputed jurisdictions, be it air, land, sea, or space defined by laws and norms rooted in geographic boundaries. The same cannot be said about cyberspace and cyber weapons. While the individuals and the hardware that power cyber weapons may be based fully within one sovereign, their actions occur in virtual space and can have real world effects across multiple sovereigns. As such, laws and norms that were designed to govern conflicts among and between nations taking place in clear geographic domains at times are ill-suited and impotent when applied to cyberattacks.

Second, in terms of weaponry, cyberattacks create tensions because their armaments of computers and computer code are frequently not designed to harm adversaries in the same manner as traditional weapons of war like foot soldiers, bombs, and bullets. What constitutes an act of war, an illegal use of force, an armed conflict, or a lesser offense if the aggression is cyber in nature? What and how should the law consider a ‘settled principles’ and ‘traditional legal tools’ developed for analogous problems in realspace.”

226. Waxman, supra note 5, at 444.
227. See Hathaway et al., supra note 5, at 827 (“Warfare traditionally functions in four domains—land, air, sea, and space—each of which is addressed by one of the full-time armed services.”).
229. See Hathaway et al., supra note 5, at 845 (discussing competing legal views on cyberattacks); Hollis, supra note 7, at 140 (highlighting difficulties of applying traditional legal doctrines to cyber attacks).
230. See, e.g., Sean Watts, Low-Intensity Cyber Operations and the Princi-
cyberattack analogous to an attack in traditional warfare? These questions are already complex for traditional operations, but become even more vexing for cyber operations relating to financial institutions and financial infrastructure. In the context of financial warfare, the intent of cyberattacks is often rooted in destabilizing and harming an adversary’s economy rather than producing human casualties. The damage is frequently financial and psychological in nature, but nonetheless devastating. For instance, in 2008, a malicious espionage software program called GhostNet was discovered in the computer system of the Dalai Lama, and later in computer systems located in over one hundred countries, including the systems of foreign ministries and embassies. GhostNet gave an outside party complete control and occupation of another party’s computer system without detection. Had GhostNet been an elite covert group of Chinese soldiers physically occupying and commandeering the information system of another country’s embassy or finance ministry towards destructive ends, the ple of Non-Intervention, in CYBERWAR, supra note 7, at 249–51; David E. Graham, Cyber Threats and the Law of War, 4 J. NAT’L SEC. L. & POL’Y 87, 90–100 (2010); Hollis, supra note 7, at 1027–28 (describing nebulous classifications for aggressions in cyberspace); Jensen, supra note 94, at 208–10 (questioning whether an attack on a nation’s computer network constitutes an illegal use of force under traditional international law).

231. See, e.g., Brown, supra note 5, at 180–82; Hathaway et al., supra note 5, at 843–46 (outlining competing perspectives on the inquiry of what constitutes a cyberattack); Hollis, supra note 228, at 180–82 (advocating for requiring “states to use cyber operations in their military operations whenever they are the least harmful means available for achieving military objectives”); Matthew J. Sklerov, Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty To Prevent, 201 MIL. L. REV. 1, 74–75 (2009); Sean Watts, Combatant Status and Computer Network Attack, 50 VA. J. INT’L L. 391, 425 (2010) (asserting that traditional laws of war that govern uses of force should govern cyber weapons as well).


233. Sanger, supra note 218.


235. See id. at 5–6; Bambauer, supra note 7, at 1014 (describing GhostNet as “a sophisticated software program capable of covertly capturing keystrokes, copying files, and even activating cameras and microphones attached to infected computers”).
rules of engagement would be relatively clear.236 However, because GhostNet is a software program likely attributable to China, the rules of engagement are not as clear.237 Attempting to map rules and norms designed for weapons and attacks that kill humans and physically destroy structures to weapons and attacks that disrupt and decimate computer systems can be incredibly difficult.238 Part of the challenge is rooted in the fact that cyberattacks can come in so many forms with a wide-range of consequences that encompasses the temporary denial of service to a website to the destruction of a nuclear weapons facility.239 As a result of these challenges, to date, there are no widely accepted treaties or norms governing the use of cyber weapons.240

Third, in terms of governance, cyberattacks have created breaks among nation-states and other stakeholders about how best to govern cyberspace. Traditional warfare and armed conflict is largely governed by over a century of established and widely agreed upon rules and norms (albeit with some disagreements).241 As previously noted, the same cannot be said about the emerging war theater of cyberspace, where key stakeholders possess competing visions of the best governance models. The United States generally prefers a multiple stakeholder model of cyber governance where states, international organizations, and private actors all play a shared role in governance.242 The Obama administration has publicly declared the United States’ commitment to “[p]romote and enhance multi-stakeholder venues for the discussion of Internet governance

236. Jensen, supra note 94, at 222.
237. See INFO. WARFARE MONITOR, supra note 234, at 48; Jensen, supra note 94, at 235–36 (contrasting the rules of engagement for traditional attacks and cyberattacks).
239. See Jensen, supra note 94, at 222; Hathaway et al., supra note 5, at 836 (asserting that “[c]yber-warfare can also constitute both cyber-attack and cyber-crime”).
240. See Hollis, supra note 7, at 135–40; Sanger, supra note 218.
241. See KENNEDY, supra note 199, at 46–63 (chronicling the historical evolution of law and war).
242. Eichensehr, supra note 7, at 321.
China and Russia, alternatively, generally prefer a sovereignty-oriented model of cyber governance that gives individual states most of the power. In fact, in early 2015, pursuant to its vision of cyberspace governance, China issued a series of regulations that gave it even greater control over the Internet as used in China, including requiring companies, particularly those working with Chinese banks, to give government regulators “backdoor” access to all computerized systems in the country; those regulations were temporarily suspended later in 2015 after much protest from American banks and other corporations. Because of these dueling visions of cyberspace governance, there exists no meaningful international consensus or accord on the governance of cyberspace and cyberattacks among key stakeholders, despite their growing prevalence and growing importance.

It is important to note that this discussion about the difficulties of mapping traditional modes of law to cyberattacks does not suggest that cyberspace is completely lawless, ungovernable, or without shared values among key stakeholders. It is understood that significant efforts have been made to expand traditional legal doctrines to the realms of cyberattacks in recent years, and that international stakeholders can reach agreements in critical areas concerning cyberattacks while maintaining strong disagreements in other areas. Internationally, NATO’s Cooperative Cyber Defence Centre of Excel-

243. WHITE HOUSE, supra note 188, at 22.
244. See Eichensehr, supra note 7, at 320.
246. See Sanger, supra note 218.
lence initiated a multi-year, multi-country study on law and cyberwarfare, which culminated in the *Tallin Manual on the International Law Applicable to Cyber Warfare* as an important compilation of guiding principles.\(^{250}\) In 2013, the United States and other countries party to the Wassenaar Arrangement, an agreement governing international arms sales, included intrusion software as a restricted dual-use technology.\(^{251}\) That same year, the United Nations also issued a report of recommendations on information and telecommunications security.\(^{252}\) Domestically, when Congress passed the 2012 National Defense Authorization Act, it stated that offensive military cyber operations would be subject to the War Powers Resolution.\(^{253}\) More broadly, the United States has taken the general position that emerging issues relating to cyberspace do “not require a reinvention of customary international law, nor [do they] render existing international norms obsolete.”\(^{254}\) Additionally, the United States has also taken the position that, to the extent that hostile cyber actions cause the same damage as traditional warfare actions, similar laws and norms concerning self-defense will govern.\(^{255}\) And in 2015, the United States and China reached a preliminary agreement concerning broad principles relating to cybersecurity.\(^{256}\) Nevertheless, despite recent preliminary ef-

\(^{250}\) NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, *TALLIN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE* (Michael N. Schmitt ed., 2013).


\(^{253}\) See National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2011). But see Jensen, *supra* note 228, at 538 (“Of course, being ‘subject to’ the WPR [War Powers Resolution] does not mean it applies. It simply means that when it applies, the Executive Branch will comply with its requirements.”).

\(^{254}\) WHITE HOUSE, *supra* note 188, at 9.

\(^{255}\) See *id.*, at 14 (“When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners.”); see also Koh, *supra* note 238, at 4 (“A state’s national right of self-defense . . . may be triggered by computer network activities that amount to an armed attack or imminent threat thereof.”).

\(^{256}\) See Memorandum of Understanding on U.S.-China Development Co-
forts and working understandings, cyberattacks nonetheless pose serious challenges for traditional laws and norms of war, as many critical issues relating to sovereignty, weaponry, and governance remain unresolved.\textsuperscript{257}

C. OF NON-STATE ADVERSARIES

Traditional laws and norms of war and armed conflict are robust and rich in addressing the actions of state adversaries, but they are not as well equipped to address the actions of non-state adversaries.\textsuperscript{258} While non-state adversaries like terrorist organizations have existed for centuries, much of the legal infrastructure remains better suited to address state adversaries.\textsuperscript{259} As non-state adversaries continue to play more prominent roles in modern warfare, tensions arise when old doctrines mismatch new realities.\textsuperscript{260} Non-state adversaries present spe-
cial challenges for the law because of the lack of meaningful comity, reciprocity, and accountability.

In terms of comity and reciprocity, nation-states can readily enter into legal agreements that govern their wartime behavior and reasonably expect one another to cooperatively abide by them.\textsuperscript{261} For instance, the Hague Conventions of 1899 banned the use of certain poisonous arms in warfare among nations.\textsuperscript{262} More recently, the United States, Japan, and a number of European nations have ratified the Council of Europe’s Convention on Cybercrime (a.k.a. The Budapest Convention) to govern actions related to the emerging field of cybercrime.\textsuperscript{263} However, unlike state actors, it is much more difficult to enter into legal agreements about wartime behavior with non-state adversaries.\textsuperscript{264} Additionally, given their lawless and barbaric behavior, it is hard to imagine hackers or terrorist groups like al Qaeda and ISIS ever reaching a formal accord or treaty with a state-based adversary like the United States.\textsuperscript{265} This discussion on the lack of comity and reciprocity does not mean to suggest that in dealing with non-state adversaries state actors should ignore all the laws and norms of war and armed conflict. Ultimately, as President Obama stated in his 2009 Nobel Lecture,\textsuperscript{266}

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{261} See ANDREW T. GUZMAN, HOW INTERNATIONAL LAW WORKS: A RATIONAL CHOICE THEORY 18 (2008) (describing how reciprocity and rational choice engenders cooperation among states); GOLNOOSH HAKIMDAVAR, A STRATEGIC UNDERSTANDING OF UN ECONOMIC SANCTIONS: INTERNATIONAL RELATIONS, LAW, AND DEVELOPMENT 136 (2014) (explaining how states generally interact on a rational basis with other states); Daphné Richemond-Barak, Applicability and Application of the Laws of War to Modern Conflicts, 23 FLA. J. INT’L L. 327, 328 (2011) (“Reciprocity’ in international law refers to the expectation by a belligerent state that other state parties to a conflict will respect similar legal and behavioral norms, such as non-use of prohibited weaponry, minimization of collateral damage, and humane treatment of prisoners of war.”).
\item \textsuperscript{262} Convention with Respect to the Laws and Customs of War on Land, with Annex of Regulations, art. 23, July 29, 1899, 32 Stat. 1803.
\item \textsuperscript{263} COUNCIL OF EUR., EUROPEAN TREATY SERIES: CONVENTION ON CYBERCRIME (2001).
\item \textsuperscript{264} See, e.g., Richemond-Barak, supra note 261 (“Non-state actors, which are not party to treaty-based norms regulating the conduct of war, cannot be assumed to operate on the basis of reciprocity.”).
\item \textsuperscript{265} See, e.g., Eichensehr, supra note 7, at 370 (“[E]ven if states agreed among themselves to restrict military activities in cyberspace, such an agreement would not restrain nonstate actors, who may already have or will almost certainly acquire military capabilities in cyberspace.”).
\end{itemize}
\end{footnotesize}
“adhering to standards, international standards, strengthens those who do, and isolates and weakens those who don’t.”

In addition to comity and reciprocity, unlike state adversaries, it is much more difficult to hold non-state adversaries accountable to wartime laws and norms. With state-based adversaries, traditional tools of international law and diplomacy can be used to hold them accountable for breaches of wartime laws and norms (albeit not always with success). Non-state adversaries like hackers, terrorists, and lone-wolf combatants are frequently much more difficult to trace and find, let alone hold accountable. If a uniformed battalion of Russian soldiers infiltrated and destroyed the servers of the New York Stock Exchange, the American and international response would likely use traditional tools of international law and diplomacy to hold Russia accountable for the battalion’s actions. However, if a nameless lone-wolf terrorist, claiming affiliation with no state and only an online movement, decides to infiltrate and destroy the servers of the New York Stock Exchange, the American and international response to hold that lone-wolf terrorist accountable would have to be more creative and break from traditional laws and norms of war given the difficulties of identifying proper avenues for retaliation. In the absence of clear international law and military mechanisms,


267. See, e.g., Blum, supra note 5, at 168–73 (discussing the equal application of international law among states); W. Michael Reisman, Assessing Claims To Revise the Laws of War, 97 AM. J. INT’L L. 82, 82 (2003); Waxman, supra note 5, at 444 (discussing accountability challenges involved with non-state actors).


270. See, e.g., Lynn, supra note 238, at 97.

271. See, e.g., id.
domestic criminal enforcement tools may be more feasible as a near term tool for such serious transgressions.

Moreover, the issue of accountability is predicated on the notion that wrongdoers can be properly identified for their misdeeds. International law generally requires the attribution of an attack to a state actor before sanctioning a responsive proportionate use of force. Further complicating matters is that many non-state adversaries can reside in locales governed by state adversaries or neutral states thereby making assistance in identifying non-state adversaries that much more difficult. For many actions by non-state adversaries, like those that use financial cyber weapons, attribution can be particularly difficult or nearly impossible with a high degree of certainty. As such, if attribution is uncertain, enforcement is frequently unachievable at a just and satisfactory level.

* * *

The world changes swiftly, and the law changes slowly. This Aesopian turtle and hare dynamic leads to tensions when old rules meet new concerns in modern warfare. Innovations at the intersection of modern war and finance exhibit this tense dynamic. The Geneva Conventions, the body of treaties gov-

272. See Sklerov, supra note 231, at 38 (“[T]he prevailing view of international law requires states to attribute an attack to a state or its agents before responding with force . . . .”).


276. See Eichensehr, supra note 221, at 358 (“New technologies pose challenges for law and for international law in particular. For as cumbersome and slow as domestic law appears in many circumstances, developing international law is often even more difficult.”).

277. See INTELLIGENCE & NAT’L SEC. ALL., supra note 94, at 6 (“National and international laws, regulations, and enforcement are still struggling to catch up to cyber activities worldwide.”); Koh, supra note 5, at 1772 (remarking on the legal challenges posed by emerging technologies).

278. See Stephen J. Choi & Andrew T. Guzman, National Laws, Interna-
erning wartime conduct, remain largely unchanged since the years following World War II, despite revolutionary changes in the world of weaponry and warfare.\textsuperscript{279} The disparate timelines of law and war create significant tensions and unanswered questions. In terms of financial warfare, answers to critical questions concerning financial hostilities, cyberattacks, and non-state adversaries remain works-in-progress and render traditional rules of law impotent to fully address the dangers of modern warfare and national security.\textsuperscript{280}

IV. KEY RECOMMENDATIONS

The new financial theater of war and its weapons demand new laws and policies so as to better protect American interests and the American homeland. In order to remain relevant, laws and policies governing war must be updated in the same way that law has historically responded to other critical social, technological, and economic changes in the past.\textsuperscript{281} While many larger legal and political questions concerning financial warfare

\begin{itemize}
  \item Hathaway et al., supra note 5, at 840.
  \item See, e.g., Eichensehr, supra note 7, at 380 (“The intersovereign issues posed by cyber are more complicated and will probably take even longer to solve.”).
  \item See ZARATE, supra note 1, at 356 (“The financial battlespace is constantly evolving . . . . Our enemies are smart and will continue to adapt, taking advantage of the growing complexity and sophistication of international financial systems. We, too, must adapt . . . .”); O.W. Holmes, The Path of the Law, 10 HARV. L. REV. 457, 474–75 (1897) (articulating the necessity of law to adapt itself to novel technology); Harold Hongju Koh, Remarks: Twenty-First Century International Lawmaking, 101 GEO. L.J. 725, 745–46 (2013) (espousing changes and breaks in international lawmakers from past customs and practices); Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, 193 (1890) (‘Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.’).
\end{itemize}
highlighted in the previous Part remain unresolved, a nation’s right to reasonably protect its financial infrastructure and financial interests from legitimate threats should not be questioned. While broader, international, and multilateral consensus remains forthcoming, domestic actions can be taken with greater urgency to better focus public and private resources on financial warfare in a coordinated manner. To better enhance financial defenses and capabilities, policymakers should introduce innovative cybersecurity incentives, advanced technological stress tests, and comprehensive financial war games to intelligently marshal public and private actors against the emerging threats posed by the financial weapons of war.

A. CYBERSECURITY INCENTIVES

Since much of modern finance operates predominantly in a privately held cyberspace infrastructure, policymakers should design incentives that encourage private businesses to expeditiously enhance their cybersecurity capabilities in response to the emerging threats of financial weapons of war. Because much of the critical financial infrastructure is owned and operated by private businesses, and because such businesses are frequently motivated by profits, carefully calibrated incentives may be necessary to spur timely cybersecurity improvements.

282. See, e.g., U.N. Charter art. 51; DEPT OF DEF. OFFICE OF THE GEN. COUNSEL, AN ASSESSMENT OF LEGAL ISSUES IN INFORMATION OPERATIONS 15–18 (1999); Jensen, supra note 94, at 230 (“International law is clear in regard to passive measures: every nation has the right to protect its computer systems by such means, just as it would its own airspace or territory.”).

283. See, e.g., ANNE-MARIE SLAUGHTER, A NEW WORLD ORDER 15–23 (2004) (arguing how emerging international issues can be better addressed through “government networks” constituted by legislators, regulators, and private stakeholders); Koh, supra note 281, at 743 (discussing the growing utility of “hybrid private-public arrangements” to address issues with international implications).

284. See, e.g., HARRIS, supra note 7, at xxii (“Defending computer networks, and launching attacks on them, requires the participation, willing or otherwise, of the private sector.”); Christopher S. Yoo, Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures, in CYBERWAR, supra note 7, at 192–93 (highlighting the need for “improved software engineering”); Sales, supra note 7, at 1550–52 (discussing the use of carrots and sticks to improve cybersecurity); Bruce P. Smith, Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help, 1 J.L. ECON. & POL’Y 171, 173 (2005).

285. See Eichensehr, supra note 7, at 350 (“[P]rivate parties own the majority of the underlying infrastructure that supports the cyber domain.”).
and investments. In the absence of incentives, investments in
cybersecurity may remain stagnant as businesses focus on their
bottom line rather than their information security and institu-
tional stability.\footnote{286}

A pure market-based approach towards cybersecurity may be
inadequate for building better defenses against dynamic
threats.\footnote{287} In the past couple of years alone, over half a billion
people had their identities stolen online, President Obama’s
credit card was breached, and the White House, the State De-
partment, Target, J.P. Morgan Chase, and Home Depot all suf-
fered serious cybersecurity breaches.\footnote{288} Despite serious and
persistent threats, it has been estimated that financial firms
only invested approximately seven percent of their information
technology budgets on security in recent years, though invest-
ments are growing in response to increased threats.\footnote{289} J.P.
Morgan Chase, for instance, invested “more than $250 million,
and had approximately 1,000 people focused on cybersecurity
efforts” in 2014 alone, expecting significantly increased invest-
ments in the near future.\footnote{290} While some companies have made
significant proactive cybersecurity investments, many have not.
And to the extent incremental improvements are made, they
are often done in a reactionary manner following some major
security breach, so policy incentives may be necessary to en-
courage more proactive and timely behavior among more pri-
vate firms.\footnote{291}

\footnote{286. See \textit{Stewart Baker et al., McAfee, In the Crossfire: Critical In-
frastructure in the Age of Cyber War} 14 (2009); \textit{NY Dep’t of Fin. Serv.,
Report on Cyber Security in the Banking Sector} 11 (May 2014) (high-
lighting resource constraints and stale software as ongoing challenges for fi-
nancial cybersecurity); Nicole Perlroth, \textit{Hacked vs. Hackers: Game On}, N.Y.
TIMES, Dec. 3, 2014, at F1 (reporting on the lack of urgency regarding
cybersecurity).}

\footnote{287. \textit{Joel Brenner, America the Vulnerable: Inside the New Threat
Matrix of Digital Espionage, Crime, and Warfare} 239 (2011).}

\footnote{288. See Perlroth, \textit{supra} note 286.}

\footnote{289. See \textit{Sales, supra} note 7, at 1538–39; Daniel Huang et al., \textit{Financial
Firms Boost Cybersecurity Funds}, WALL. ST. J., Nov. 17, 2014, at C3.}

\footnote{290. See JPMorgan Chase & Co., \textit{Annual Report (Form 10-K)}, at 142 (Feb.
24, 2015); JPMorgan Chase & Co., \textit{Quarterly Report (Form 10-Q)}, at 66 (Aug.
3, 2015) (“In each of 2015 and 2016, the Firm expects its annual cybersecurity
spending to be nearly double what it was in 2014 in order to enhance its de-
fense capabilities.”).}

\footnote{291. Huang et al., \textit{supra} note 289; Jessica Silver-Greenberg & Matthew
Goldstein, \textit{After Breach, Push To Close Security Gaps}, N.Y. TIMES, Oct. 22,
2014, at B1; see, e.g., Derek E. Bambauer, \textit{Schrödinger’s Cybersecurity}, 48 U.C.
DAVIS L. REV. 791, 848–50 (2015) (discussing various political tools for encour-}
Tax law, if properly calibrated, can serve as one such incentive-oriented policy to encourage private financial industry actors to enhance their cyber defenses in a timely manner. Through a combination of tax credits, bonus depreciation, and increased deductions, policymakers can encourage the replacement of outdated, vulnerable information systems and greater investment in better, more secured systems. Following the recent financial crisis, pursuant to the American Recovery and Reinvestment Act, policymakers used tax policy to incentivize private businesses to accelerate and enlarge capital investments to help stimulate the economy. Similarly, such incentive-driven policies can be utilized to motivate private financial industry participants to act more expediently towards enhancing cybersecurity as a part of enhancing American financial security.

Beyond tax policy, the federal government can also create better incentives through its vast procurement powers. The federal government can become a more active and public buyer or sponsor in the growing market for cyber weapons, cyber defenses, and so-called zero-day exploits, which are vulnerabilities unknown to a program’s administrator. If direct, open


295. See, e.g., Derek E. Bambauer & Oliver Day, The Hacker’s Aegis, 60 Emory L.J. 1051, 1067–68 (2011) (discussing the growing market for cyber weapons and cyber defenses); Grossman, supra note 164, at 20–21 (reporting on the market for computer bugs, viruses, and vulnerabilities); Serena Saitto, The Big Business of Smashing Bugs, Bloomberg Businessweek, Mar. 16, 2015, at 41 (highlighting the rise of the "bug bounty" marketplace).
federal government participation is too controversial, the federal government can also offer certain benefits or subsidies to those who sell exclusively to the American government or legitimate, white-hat American corporations. Private firms like Google and Microsoft already participate in this cyber arms marketplace. It has been documented that Google is willing to pay sums up to $60,000 for vulnerabilities in its Chrome browser; and Microsoft is willing to pay up to $100,000 for vulnerabilities in its software programs. The participation of the federal government, directly or indirectly, through mechanisms like prizes and bounties in this marketplace could help assure that these cyber arms are not unleashed on American financial interests.

In addition to participating in the market for cyber weapons through its procurement powers, the federal government can also encourage timely cybersecurity improvements by private financial firms by expressing a contracting preference for firms that meet certain government cybersecurity benchmarks, if those benchmarks are regularly updated to be responsive to the current threats in cyberspace. Because the federal government is one of the largest purchasers of goods and services in the world, such contracting preferences could lead to significant system-wide improvements in cybersecurity. The federal government already has cybersecurity requirements for many of its vendors, but it can do more to make sure that its cybersecurity requirements reflect the latest cyberthreats. In fact, in 2015, the Office of Management and Budget initiated a review of current acquisition practices with an eye towards enhancing cybersecurity through the federal procurement process.

296. See, e.g., Bambauer, supra note 7, at 1087–88 (advocating for a government “bug bounty” program to purchase computer viruses and other malicious software).
297. See ZETTER, supra note 178, at 100.
298. Id. at 102.
299. See, e.g., Bambauer, supra note 7, at 1062–63 (suggesting implementation of IT requirements as a condition of contracting with the government); see also BAKER ET AL., supra note 286 (discussing underinvestment by private firms in cybersecurity).
300. See Bambauer, supra note 7, at 1062–63; Gitterman, supra note 294 (examining the power of the president to shape policy using procurement).
302. Improving Cybersecurity Protections in Federal Acquisitions Public Comment Space, OFFICE OF MGMT. & BUDGET, https://policy.cio.gov (last visit-
While the threats of cyberattacks are well known in the financial industry, the common business instincts to increase earnings and decrease expenditures may prevent businesses from behaving in the proactive and timely manner that is most beneficial to them and to the entire financial system. It may be necessary for the government to initiate and coordinate some of the desired outcomes. Proper public policy incentives could mitigate some of the collective action problems associated with cybersecurity. Moreover, because private enterprises play such critically important roles in modern finance, enhancements of our national cybersecurity without complementary private enhancements would be incomplete, and would leave the homeland very vulnerable to various financial weapons of war. As such, incentive-oriented policies may be necessary to improve the overall security of the financial system.

B. TECHNOLOGICAL STRESS TESTS

Policymakers should design advanced technological stress tests to assess the information technology infrastructure of systemically important private and public financial institutions and agencies. These tech stress tests should be constructed and implemented to analyze the capabilities and vulnerabilities of the information technology systems of these entities similar to how banking regulators imposed capital stress tests to large financial institutions following the financial crisis. They can be administered through a federal agency apparatus like the Department of Homeland Security’s National Cybersecurity and
Communications Integration Center. These tests can help address some of the informational challenges associated with cybersecurity. They can provide policymakers and key industry stakeholders with a more holistic, mosaic view of the cyberthreats being experienced by the financial system rather than just seeing glimpses of the threats based on firm-by-firm disclosures. The proposed technological stress tests can also create more opportunities for firms to share information and learn from one another. The fact of the matter is that in an age of persistent cyberattacks, no technological defense is failsafe and no weapon can serve as a complete deterrence. As such, private and public financial stakeholders must periodically learn about their own vulnerabilities as well as system-wide vulnerabilities so as to build better defenses.

The recommendation of advanced technological stress tests is neither radical nor wholly unprecedented. The Pentagon and many financial institutions already voluntarily, or as part of legal requirements, conduct some periodic testing with regards to their cybersecurity. Plus, the law also already requires many financial institutions to meet certain minimum informational safeguards. Pursuant to the 1998 Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators, the financial industry established the Financial Sector-Information Sharing and Analysis Centers to help aggregate and share information about cybersecurity threats. The Fi-


309. See Bambauer, supra note 7, at 1035 (explaining how information asymmetries are obstacles for better cybersecurity).

310. See FIN. INDUS. REGULATORY AUTH., supra note 156, at 34–36.

311. See Eichensehr, supra note 7, at 367 (opining that no state has a fail-safe technological infrastructure); Lynn, supra note 298, at 97; Nye, supra note 269.


nancial Services Modernization Act of 1999 mandates that regulated institutions meet certain benchmarks for protecting the financial information of their customers.\textsuperscript{314} Similarly, the Pentagon also runs annual tests on all of its major weapon systems, including assessments for cybersecurity.\textsuperscript{315} More recently, in 2014, the Financial Industry Regulatory Authority also recommended third-party penetration testing for financial firms as a way to assess their cybersecurity feasibility and vulnerability.\textsuperscript{316} And in 2015, collectives of private firms created platforms like Soltra and ThreatEx to share information about cyberthreats.\textsuperscript{317}

In recognition of the persistent and growing threats of cyber weapons to our critical infrastructure, policymakers have recently taken more steps to enhance our cybersecurity capabilities. In 2013, Congress introduced the Cyber Intelligence Sharing and Protection Act to enhance the cyber infrastructure of the country, particularly the parts that are controlled by private firms who are less likely to work together.\textsuperscript{318} Because that bill did not become law, President Obama signed an executive order focused on improving the cybersecurity of our nation’s critical infrastructure.\textsuperscript{319} As previously noted, the executive order, among other matters, established the U.S. National Institute for Standards and Technology Cybersecurity Framework to encourage more collaboration and information sharing among public and private stakeholders on best practices in cybersecurity.\textsuperscript{320} Given the importance of our financial system, efforts to better protect our critical infrastructure from cyberattacks should include our financial infrastructure and its

\begin{footnotesize}
\begin{itemize}
\item[315.] ODOTE, supra note 161, at 331–37.
\item[316.] See FIN. INDUS. REGULATORY AUTH., supra note 156, at 34 (highlighting the importance of information sharing in cybersecurity).
\item[318.] Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013).
\item[320.] NAT'L INST. OF STANDARDS & TECH., IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY EXECUTIVE ORDER 13636: PRELIMINARY CYBERSECURITY FRAMEWORK I (2013).
\end{itemize}
\end{footnotesize}
key participants. And advanced technological stress tests can be a step in that direction.

In the aftermath of the financial crisis, large financial institutions with assets over $50 billion in the United States were subject to capital stress tests to assess the adequacy of their reserves in the event of another financial crisis. These financial institutions were subject to a host of hypothetical adverse economic and financial scenarios to test their vulnerability and viability under certain hypothetical dire circumstances. These hypothetical nightmare scenarios include a parade of economic horrors like sudden drops in gross domestic product, spikes in unemployment, and crashes in housing prices. The Federal Reserve and the relevant financial institutions conducted these stress tests under the auspices of the Supervisory Capital Assessment Programs (SCAP), Comprehensive Capital Analysis and Review (CCAR), and Dodd-Frank Act stress testing (DFAST), which were all implemented following the financial crisis. Foreign banking regulators have also implemented similar stress tests for their systemically important financial institutions. These stress tests, while imperfect, can nonetheless provide valuable information for policymakers and tested financial institutions.


326. See Policy Statement on Scenario Design Framework for Stress Test-
Because the modern financial industry is essentially a high-tech industry, stress tests akin to those that test capital adequacy should be conducted to test the technological capabilities and vulnerabilities of our critical financial institutions and agencies when subject to adverse technological situations. Similar to the capital stress tests, the detailed results of these tests will remain confidential so that vulnerabilities within an institution or the system are not disclosed to our adversaries. Like the capital stress tests, the technological stress tests will include large financial institutions like investment banks, but also critically important financial infrastructure participants like stock exchanges, mutual funds, and clearinghouses. Additionally, unlike the capital stress tests, the key financial regulators such as the Federal Reserve, the SEC, the Financial Industry Regulatory Authority, the Treasury Department, and the Labor Department would also be subject to these technological stress tests because of their systemic importance and because they may have unknown vulnerabilities. In fact, in recent years, mindful of potential cyber breaches of confidential financial information, major financial institutions have bolstered their own technological defenses and have also encouraged their outside law firms to enhance their cybersecurity. Ultimately, because of the interconnected nature of the modern financial system and its heavy dependence on information technology, it is imperative that critical institutions are technologically well-
equipped to handle technological stresses and threats from foreign and domestic adversaries.\(^{329}\)

C. WAR GAMES

Policymakers should design comprehensive military exercises that include serious threats to the American financial system and American financial interests to better prepare for modern conflicts and warfare.\(^{330}\) These war games should marshal military resources, as well as private resources to participate in these exercises. The Departments of Defense, Homeland Security, and Treasury can serve as the leading and coordinating agencies for these exercises that involve public agencies as well as private institutions. The participation of private institutions is critically important to having effective war games because private firms play such an important role in the global financial infrastructure and in financial warfare.\(^{331}\) Private firms like banks, clearinghouses, and exchanges are at the frontlines of the financial theater of war, and they can certainly play a more active role in enhancing our national security readiness and our recovery capabilities.\(^{332}\) Just as war games have long assisted the military in preparing for conflict in the theaters of land, air, and sea, these war games can help the military and private firms better prepare for conflicts in the financial theater of war.\(^{333}\) Whereas the technological stress tests are

---

\(^{329}\) See Eichensehr, supra note 7, at 368 (“[I]ncreased investment in and dependence on the Internet and cyber more generally increase a state’s vulnerability to attack.”).

\(^{330}\) Professor Mehrsa Baradaran has proposed using financial war games, in addition to stress tests, to better assess the strengths and weaknesses of financial institutions. See Baradaran, supra note 6, at 1319; see also John Crawford, Wargaming Financial Crises: The Problem of (In)experience and Regulator Expertise, 34 REV. BANKING & FIN. L. 115, 168–74 (2014) (describing various benefits of using financial crises simulations).

\(^{331}\) See Gordon, supra note 135, at 510–17 (explicating on the important role of private firms in combatting terrorism financing); Sales, supra note 7, at 1567 (“[T]he private sector should play an active role in establishing industry-wide cyber-security standards . . . .”); Matthew Goldstein, Wall St. and Law Firm Plan Cooperative Body To Bolster Online Security, N.Y. TIMES, Feb. 24, 2015, at B7; see also DEP’T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 8–9 (2011) (advocating for more partnerships between the public agencies and the private sector to enhance cybersecurity).

\(^{332}\) See, e.g., Baradaran et al., supra note 1, at 515–23 (suggesting that American financial institutions can do significantly better to detect and deter funding for terrorism).

\(^{333}\) For an introduction to the role of war games throughout history, see generally FRANCIS J. MCHUGH, FUNDAMENTALS OF WARGAMING (3d ed. 1966); PETER P. PERLA, THE ART OF WARGAMING (1990); JON PETERSON, PLAYING AT
primarily structured, targeted exercises, the proposed war games would be comprehensive operational exercises that account for analog weapons as well as cyber weapons with considerably less predictability and more unintended scenarios. If properly designed, financial war games better prepare policymakers to anticipate the complexities surrounding financial warfare.\footnote{THE WORLD: A HISTORY OF SIMULATING WARS, PEOPLE AND FANTASTIC ADVENTURES, FROM CHESS TO ROLE-PLAYING GAMES (2012).}

War games have long been used by militaries, here and abroad, to enhance readiness and national defenses.\footnote{See, e.g., Robert C. Rubel, The Epistemology of War Gaming, 59 NAVAL WAR C. REV. 108, 112 (2006) (“Games allow players and observers to see relationships—geographic, temporal, functional, political, and other—that would otherwise not be possible to discern. Seeing and understanding these relationships prepares the mind for decisions in a complex environment.”).} Early variations of chess date back to 3000 B.C. and were considered to be one of the first forms of war games.\footnote{See Baradaran, supra note 6, at 1319 (“The military has used war games for many years, both as a test of the military’s responsiveness to crises and as a way to devise military strategies.”).} War games simulate potential threats and attacks in a semi-controlled environment where its participants can better learn about their strengths and vulnerabilities in a dynamic setting.\footnote{See MCHUGH, supra note 333, at 27.} During the Cold War, the Pentagon ran a series of hypothetical and operational exercises to test the efficacy of the U.S. military in connection to certain adverse scenarios occurring in Europe and Asia.\footnote{DEPT OF DEF., JOINT PUBLICATION 1-02: DICTIONARY OF MILITARY AND ASSOCIATED TERMS 395 (2011) (defining a war game as “[a] simulation, by whatever means, of a military operation involving two or more opposing forces, using rules, data, and procedures designed to depict an actual or assumed real life situation”).} Since 1982, the United States and Thailand have spearheaded large-scale operational war games called Cobra Gold, which presently includes Indonesia, Japan, Malaysia, Singapore, and South Korea.\footnote{Thomas B. Allen, Twilight Zone in the Pentagon, in THE COLD WAR: A MILITARY HISTORY 230, 230–34 (Robert Cowley ed., 2005).} More recently, in connection with emerging threats posed by China and North Korea, the United States and South Korea also run one of the largest full-scale military exercises called Foal Eagle annually to test their readiness.\footnote{Ralf Emmers, Security and Power Balancing: Singapore’s Response to the US Rebalance in Asia, in THE NEW US STRATEGY TOWARDS ASIA 143, 146 (William T. Tow & Douglas Stuart eds., 2015).}
Approximately 10,000 U.S. troops from the Army, Navy, Air Force, and Special Operations Forces were involved in the 2013 Foal Eagle war games alone.\textsuperscript{341}

As the nature of war evolves to include more non-state adversaries, cyber weapons, and analog financial weapons, the military must work closer with key private institutions to design war games that better prepare for attacks that attempt to disrupt and destroy our financial system and financial interests.\textsuperscript{342} Osama Bin Laden did not choose to attack the World Trade Center in New York City by accident. He chose the Twin Towers and New York City because of their economic and financial importance to the United States.\textsuperscript{343} These war games should account for tactics like coordinated economic sanctions by competing nation-states, attacks to disrupt our financial infrastructure, efforts to manipulate our capital markets, schemes to decimate our economic strength, and attempts to physically destroy our financial institutions. Financial war games can help us think like the enemy.\textsuperscript{344} They can help our military, law enforcement, and private institutions prepare for terrorists using alternative funding sources like peer-to-peer lending, bitcoins, and crowdfunding to finance their activities.\textsuperscript{345} Financial war games can also help our military prepare for horrific scenarios like the seizure of American banking interests abroad, the commandeering of the New York Stock Exchange servers, the injection of false data into our bond markets, a sudden, massive sale of U.S. Treasury bonds, and the bombing of major investment banks in New York. Through significantly realistic simulated scenarios, war games can provide incredibly valuable intelligence to public policymakers and private firms of their strengths and vulnerabilities.\textsuperscript{346}

\textsuperscript{341} Id.

\textsuperscript{342} See Dep't of Def., supra note 94, at 2 (discussing the core missions of the Department of Defense including defending the United States against cyberattacks that may have significant economic and financial consequences).


\textsuperscript{344} See generally Micah Zenko, Red Team: How To Succeed By Thinking Like The Enemy (2015).

\textsuperscript{345} See, e.g., Rick Rojas & Ian Lovett, Buyer of Guns Used in Attack Is Studied, N.Y. Times, Dec. 9, 2015, at A14 (reporting on how the terrorists in the 2015 San Bernardino attack used online peer-to-peer lending site, Proper, to arrange for a loan).

\textsuperscript{346} See, e.g., U.S. Gov't Accountability Office, supra note 116, at 34–
This proposal for comprehensive operational financial war games that includes private and public sector actors is not entirely unprecedented. Mindful of the utility of war games in connection with financial weapons, in 2009, the U.S. military and intelligence officials conducted one of the first reported economic war games at the Johns Hopkins University Warfare Analysis Laboratory in Laurel, Maryland, to test the use of financial weapons against the United States by a foreign nation like China.  

Recent efforts like the National Cyber-Forensics & Training Alliance, a non-profit corporation established by the Federal Bureau of Investigation to marshal public and private sector resources to share information, expertise, and resources to combat threats to cybersecurity, may serve as a good model for designing more comprehensive financial war games. Since 2011, the Securities Industry and Financial Markets Association has been running major cyberattack simulations called Quantum Dawn with private partners and federal agencies to better prepare the financial industry against a systemic cyberattack.

While no war game can perfectly simulate an actual war, a good war game can nonetheless be incredibly illuminating in helping public and private institutions better plan for financial warfare, so that they do not react in a rash, ad-hoc manner during times of crisis. As former President and General Dwight Eisenhower famously remarked about war preparations: “In preparing for battle I have always found that plans are useless, but planning is indispensable.” To date, it is difficult to say

347. WEINER, supra note 17, at 13–14.
351. RICHARD M. NIXON, SIX CRIMES 235 (1982) (quoting Dwight Eisenhower-
that we cannot plan better, or do more, to protect our homeland and our financial interests from potential and persistent attacks from our enemies with financial weapons of war. And comprehensive financial war games that marshal public and private resources in design and operation can serve as a meaningful early step towards creating better defenses against cyber weapons and analog weapons in modern financial warfare.

CONCLUSION

Financial warfare will be one of the most pressing challenges for political leaders, military commanders, financial regulators, and corporate executives in the near future. The emergence and confluence of analog and cyber financial weapons will pose some of the most vexing and daunting threats for law and society in the coming years. Every nation-state, every major financial institution, and every citizen could be at risk of suffering direct harms and collateral damage.

This Article provides an early exploration of modern financial warfare. It examines the new battlefield of the modern financial infrastructure, classifies the growing arsenal of financial weapons, highlights emerging legal and policy tensions, and offers three pragmatic recommendations for better safeguarding the homeland and the global financial system in current and future financial wars. Throughout its analysis, this Article is mindful of the longstanding international legal considerations involved with war and finance, but it is also aware of the critical need for swift and thoughtful actions to better protect American interests. In the end, this Article aspires to serve as an early, optimistic blueprint for further study on how best to think and act anew with urgency about modern financial warfare and the financial weapons of war.

352. See, e.g., U.S. GOVT ACCOUNTABILITY OFFICE, GAO-16-294, INFORMATION SECURITY: DHS NEEDS TO ENHANCE CAPABILITIES, IMPROVE PLANNING, AND SUPPORT GREATER ADOPTION OF ITS NATIONAL CYBERSECURITY PROTECTION SYSTEM 16–31 (2016); Gable, supra note 14, at 118 (“Although states, private industry, and international organizations have made significant efforts to increase international cooperation, much more needs to be done.”); Lew, supra note 176.

353. See DELOITTE, THIS IS NOT A TEST: HOW SIMULATIONS AND WARGAMING CAN HELP YOU MANAGE BUSINESS RISK AND MAKE DECISIONS IN A COMPLEX ENVIRONMENT 7 (2013).