

2016

# Financial Weapons of War

Tom C.W. Lin

Follow this and additional works at: <https://scholarship.law.umn.edu/mlr>



Part of the [Law Commons](#)

---

## Recommended Citation

Lin, Tom C.W., "Financial Weapons of War" (2016). *Minnesota Law Review*. 205.  
<https://scholarship.law.umn.edu/mlr/205>

This Article is brought to you for free and open access by the University of Minnesota Law School. It has been accepted for inclusion in Minnesota Law Review collection by an authorized administrator of the Scholarship Repository. For more information, please contact [lenzx009@umn.edu](mailto:lenzx009@umn.edu).

---

---

## Article

# Financial Weapons of War

Tom C.W. Lin<sup>†</sup>

### INTRODUCTION

Finance may be the most powerful weapon of war.<sup>1</sup> It moves armadas, armies, and squadrons. It funds troops and artillery. It endows suicide bombs and improvised explosive devices.<sup>2</sup> 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.<sup>3</sup>

---

<sup>†</sup> Associate Professor of Law, Temple University Beasley School of Law. Many thanks to Kenneth Anderson, Derek Bambauer, Gary Brown, Rebecca Crotofof, 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.

1. See, e.g., IAN BREMMER & CLIFF KUPCHAN, TOP RISKS 2015 8–9 (2015) (discussing the weaponization of finance); NICK RIDLEY, TERRORIST FINANCING: THE FAILURE OF COUNTER MEASURES 1 (2012) (asserting that money is an “essential component” of terrorist organizations); JUAN C. ZARATE, TREASURY’S WAR: THE UNLEASHING OF A NEW ERA OF FINANCIAL WARFARE 1 (2013) (“[M]oney is what fuels the operations of the world’s rogues.”); Shima Baradaran et al., *Funding Terror*, 162 U. PA. L. REV. 477, 480–82 (2014) (describing the sums of financing needed by terrorist organizations).

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.<sup>4</sup> 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,<sup>5</sup> finance,<sup>6</sup> and cyberspace,<sup>7</sup> this Article seeks to fill

---

TERRORIST FINANCING 7 (2008), <http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf> (“Funds are required to promote a militant ideology, pay operatives and their families, arrange for travel, train new members, forge documents, pay bribes, acquire weapons, and stage attacks.”); JIMMY GURULE, UNFUNDING TERROR: THE LEGAL RESPONSE TO THE FINANCING OF GLOBAL TERRORISM 3 (2008) (highlighting the importance of finance in the war on terrorism).

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

5. See, e.g., Gabriella Blum, *On a Differential Law of War*, 52 HARV. INT’L L.J. 163 (2011); Davis Brown, *A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT’L L.J. 179 (2006); Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817 (2012); Neal K. Katyal & Laurence H. Tribe, *Waging War, Deciding Guilt: Trying the Military Tribunals*, 111 YALE L.J. 1259 (2002); Harold Hongju Koh, *The State Department Legal Adviser’s Office: Eight Decades in Peace and War*, 100 GEO. L.J. 1747 (2012); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT’L L. 421 (2011); Jeffrey T. G. Kelsey, Note, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV. 1427 (2008).

6. See, e.g., Mehrsa Baradaran, *Regulation by Hypothetical*, 67 VAND. L. REV. 1247 (2014); Kathryn Judge, *Fragmentation Nodes: A Study in Financial Innovation, Complexity, and Systemic Risk*, 64 STAN. L. REV. 657 (2012); Tom C.W. Lin, *The New Investor*, 60 UCLA L. REV. 678 (2013); Jonathan R. Macey & Maureen O’Hara, *From Markets to Venues: Securities Regulation in an Evolving World*, 58 STAN. L. REV. 563 (2005); Saule T. Omarova, *The Merchants of Wall Street: Banking, Commerce, and Commodities*, 98 MINN. L. REV. 265 (2013); Steven L. Schwarcz, *Systemic Risk*, 97 GEO. L.J. 193, 200–04 (2008); Hal S. Scott, *The Reduction of Systemic Risk in the United States Financial System*, 33 HARV. J.L. & PUB. POL’Y 671, 673–79 (2010); Charles K. Whitehead, *Reframing Financial Regulation*, 90 B.U. L. REV. 1 (2010).

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.<sup>8</sup> 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.<sup>9</sup> It then identifies systemic risks, discrete vulnerabilities, and a lineup of potential adver-

---

INTERNET COMPLEX (2014); Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011 (2014); Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317 (2015); Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998); Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023 (2007); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999); Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. L. REV. 1503 (2013).

8. See *infra* Part III.A.

9. See *infra* Part I.

---

saries in this financial theater of war. Part I provides a sweeping survey of the emerging financial battlefield.

Moving from general to specific, Part II highlights particular armaments of financial warfare. Rather than provide an exhaustive catalog of financial weapons, it offers a broad inventory of the financial weapons of war. It classifies the financial weapons of war as analog weapons and cyber weapons. It accounts for traditional weapons like economic sanctions, anti-money laundering regulations, and banking restrictions, as well as digital weapons like distributed denial-of-service attacks, data manipulation hacks, and destructive intrusions.<sup>10</sup> It explains how these analog and cyber weapons are used in current 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 modern financial warfare.

Part III contends with new concerns. It asserts that the financial weapons of war present critical challenges for traditional laws and norms relating to financial hostilities, cyberattacks, and non-state actors.<sup>11</sup> It argues that certain traditional rules that governed finance and war in the past are ill-suited for a fundamentally different present, and a dramatically 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 fundamental 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 innovative cybersecurity incentives, advanced technological stress tests, and comprehensive financial war games to better prepare for threats in the financial theater of war.<sup>12</sup> Part IV suggests immediate forward steps to be seriously considered while larger policy and legal disagreements are being deliberated 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-

---

10. *See infra* Part II.

11. *See infra* Part III.

12. *See infra* Part IV.

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.<sup>13</sup> 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.<sup>14</sup> 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.<sup>15</sup> In this new battlefield, instead of bombs and bullets, the weapons of choice are financial and economic in nature.<sup>16</sup> This new battlefield is the result of advances and developments in information technology, geopolitics, and financial regulation over the last half century.<sup>17</sup> 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.”).

15. See, e.g., Annie Lowrey, *Aiming Financial Weapons from Treasury War Room*, N.Y. TIMES, June 4, 2014, at B1 (quoting Secretary of the Treasury Jacob Lew, who describes financial warfare as “a new battlefield for the United States”).

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.<sup>18</sup> 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.<sup>19</sup> Contemporary financial participants and products operate in a complex, expansive global network that connects and crosses institutions, industries, individuals, and instruments across the world.<sup>20</sup> 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.<sup>21</sup> 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-

---

WEALTHY NATIONS AND INVESTORS SECRETLY DOMINATE THE WORLD 17–25 (2010).

18. See, e.g., Tom C.W. Lin, *Infinite Financial Intermediation*, 50 WAKE FOREST L. REV. 643, 645–50 (2015) (discussing the core functions of financial intermediation).

19. See 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.”).

20. See, e.g., IAN GOLDIN & MIKE MARIATHASAN, *THE BUTTERFLY DEFECT: HOW GLOBALIZATION CREATES SYSTEMIC RISKS, AND WHAT TO DO ABOUT IT* 39 (2014) (“The global financial system has become more interconnected than ever before over the past decade due to policy and regulatory changes that have opened markets combined with the massive surge in computer power . . . .”); MARTIN WOLF, *THE SHIFTS AND THE SHOCKS: WHAT WE’VE LEARNED—AND HAVE STILL TO LEARN—FROM THE FINANCIAL CRISIS* 182–88 (2014) (discussing various linkages in the global financial system); Frank Partnoy, *Financial Innovation in Corporate Law*, 31 J. CORP. L. 799, 800 (2006) (describing the proliferation of new financial instruments).

21. See HAL S. SCOTT, *COMM. ON CAPITAL MKTS. REGULATION, INTERCONNECTEDNESS AND CONTAGION* (2012); Markus K. Brunnermeier, *Deciphering the Liquidity and Credit Crunch 2007–2008*, 23 J. ECON. PERSPS. 77, 96–98 (2009) (discussing the financial system’s “interwoven network of financial obligations”); Robin Greenwood & David S. Scharfstein, *How To Make Finance Work*, HARV. BUS. REV., Mar. 2012, at 107; Tom C.W. Lin, *Reasonable Investor(s)*, 95 B.U. L. REV. 461, 493–94 (2015) (noting that many “new investment opportunities are linked in a complex, global web of interdependent institutions and instruments frequently governed by crosscutting bodies of law that span multiple jurisdictions and regulators.”).

cludes investment banking, commercial banking, lending, market-making, trading, clearing, custodial servicing, and prime brokering.<sup>22</sup> 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.<sup>23</sup> 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.<sup>24</sup> 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.<sup>25</sup>

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.<sup>26</sup> This was made bluntly evident during the recent financial crisis when volatility in the American markets for collateralized debt obligations and mortgage-backed se-

---

22. See JPMorgan Chase & Co., Annual Report (Form 10-K) (Feb. 28, 2013).

23. Paul Glasserman & Bert Loudis, *A Comparison of U.S. and International Global Systemically Important Banks*, OFF. FIN. RES. BRIEF SERIES 15-07, Aug. 4, 2015, at 2–3.

24. See, e.g., STAFF OF S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 113TH CONG., REP. ON WALL STREET BANK INVOLVEMENT WITH PHYSICAL COMMODITIES (Comm. Print 2014); Nathaniel Popper & Peter Eavis, *Senate Report Finds Banks Can Influence Commodities*, N.Y. TIMES, Nov. 20, 2014, at B1.

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 Begets High Speed Regulation: SEC Response to Flash Crash, Rash*, 2010 U. ILL. J.L. TECH. & POL’Y 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”).

curities caused significant stress on the global financial system.<sup>27</sup> 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.<sup>28</sup>

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.<sup>29</sup> Complimentary advances in technology and regulation over the last five decades have remade the inner and outer workings of the financial system.<sup>30</sup> Technological advances made computing power and capacity exponentially better, faster, smaller, cheaper, and more readily accessible for everyone, including financial institutions.<sup>31</sup> An Apple iPhone

---

27. See, e.g., Brett McDonnell, *Don't Panic! Defending Cowardly Interventions During and After a Financial Crisis*, 116 PENN ST. L. REV. 1, 7–16 (2011) (explaining the deleterious economic impact of collateralized debt obligations and mortgage-backed securities during the financial crisis); Kenneth E. Scott & John B. Taylor, Opinion, *Why Toxic Assets Are So Hard To Clean up*, WALL ST. J., July 20, 2009, at A13.

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.

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 (Iftexhar 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.”).

30. For a general discussion about the evolution of modern finance, see Robert DeYoung, *Safety, Soundness, and the Evolution of the U.S. Banking Industry*, 92 FED. RES. BANK ATLANTA ECON. REV. 41, 41 (2007); Tom C.W. Lin, *The New Financial Industry*, 65 ALA. L. REV. 567, 572–76 (2014); Loretta J. Mester, *Commentary: Some Thoughts on the Evolution of the Banking System and the Process of Financial Intermediation*, 92 FED. RES. BANK ATLANTA ECON. REV. 67, 67–72 (2007); Arthur E. Wilmarth, Jr., *The Transformation of the U.S. Financial Services Industry, 1975–2000: Competition, Consolidation, and Increased Risks*, 2002 U. ILL. L. REV. 215, 215.

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.<sup>32</sup> Along a similar timeline, regulatory developments like Regulation Alternative Trading System,<sup>33</sup> Regulation National Market System,<sup>34</sup> and decimalization<sup>35</sup> spurred the growth of electronic communication networks and alternative trading platforms that linked financial markets all across the globe.<sup>36</sup> 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.<sup>37</sup> 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-

---

and low communication costs have expanded markets . . . ."); Chip Walter, *Kryder's Law*, SCI. AM., Aug. 2005, at 32.

32. MICHIO KAKU, PHYSICS OF THE FUTURE: HOW SCIENCE WILL SHAPE HUMAN DESTINY AND OUR DAILY LIVES BY THE YEAR 2100 21 (2011).

33. See Regulation ATS, 17 C.F.R. § 242.300(a) (2015); SAL ARNUK & JOSEPH SALUZZI, BROKEN MARKETS: HOW HIGH FREQUENCY TRADING AND PREDATORY PRACTICES ON WALL STREET ARE DESTROYING INVESTOR CONFIDENCE AND YOUR PORTFOLIO 68–78 (2012); BRIAN R. BROWN, CHASING THE SAME SIGNALS: HOW BLACK-BOX TRADING INFLUENCES STOCK MARKETS FROM WALL STREET TO SHANGHAI 2 (2010); DAVID J. LEINWEBER, NERDS ON WALL STREET: MATH, MACHINES, AND WIRED MARKETS 31–64 (2009).

34. See 17 C.F.R. § 242.601 (2015); Regulation NMS, Exchange Act Release No. 49325, 69 Fed. Reg. 11,126, 11,160 (Mar. 9, 2004); see also SCOTT PATTERSON, DARK POOLS: HIGH-SPEED TRADERS, A.I. BANDITS, AND THE THREAT TO THE GLOBAL FINANCIAL SYSTEM 49 (2012); Laura Nyantung Beny, *U.S. Secondary Stock Markets: A Survey of Current Regulatory and Structural Issues and a Reform Proposal to Enhance Competition*, 2002 COLUM. BUS. L. REV. 399, 426 (“[T]he express purpose of the NMS [is] to promote efficiency and competition across secondary markets.”).

35. See SEC. & EXCH. COMM’N, REPORT TO CONGRESS ON DECIMALIZATION 4 (2012) (“Prior to implementing decimal pricing in April 2001, the U.S. equity market used fractions as pricing increments, and had done so for hundreds of years.”); CHRISTOPHER STEINER, AUTOMATE THIS: HOW ALGORITHMS CAME TO RULE OUR WORLD 185 (2012) (discussing how decimalization bolsters electronic trading volumes and profits).

36. See ARNUK & SALUZZI, *supra* note 33.

37. See, e.g., LEINWEBER, *supra* note 33 (chronicling the rise of new, electronic financial markets); Macey & O’Hara, *supra* note 6, at 563 (“Advances in technology, combined with the dramatic decrease in the cost of information processing, have conspired to change the way that securities transactions occur.”); Saule T. Omarova, *Wall Street As Community of Fate: Toward Financial Industry Self-Regulation*, 159 U. PA. L. REV. 411, 430 (2011) (describing finance as “[a]n increasingly complex marketplace, [with] dependence on fast-changing technology”); Felix Salmon & Jon Stokes, *Bull vs. Bear vs. Bot*, WIRED, Jan. 2011, at 90 (“It’s the machines’ market now; we just trade in it.”).

form those tasks exponentially faster, cheaper, and in a more user-friendly manner.<sup>38</sup> 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.<sup>39</sup> Autonomous supercomputers assist financial institutions in assessing risk and managing assets.<sup>40</sup> Online brokerages and automated wealth managers empower retail investors to participate in finance like never before.<sup>41</sup> 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.”<sup>42</sup> 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.<sup>43</sup> 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.<sup>44</sup> Our currency is the reserve currency of the world, and the most trusted investment during

---

38. See Lin, *supra* note 18, at 653–54.

39. See PATTERSON, *supra* note 34, at 46; Frank J. Fabozzi et al., *High-Frequency Trading: Methodologies and Market Impact*, 19 REV. FUTURES MKTS. 7, 8–10 (2011); Graham Bowley, *Fast Traders, in Spotlight, Battle Rules*, N.Y. TIMES, July 18, 2011, at A1.

40. See Erik F. Gerding, *Code, Crash, and Open Source: The Outsourcing of Financial Regulation to Risk Models and the Global Financial Crisis*, 84 WASH. L. REV. 127, 130–35 (2009); Sheelah Kolhatkar & Sree Vidya Bhaktavatsalam, *The Colossus of Wall Street*, BLOOMBERG BUSINESSWEEK, Dec. 13, 2010, at 62; *The Rise of BlackRock*, THE ECONOMIST, Dec. 7, 2013, at 13.

41. See ANN C. LOGUE, DAY TRADING FOR DUMMIES 196 (3d ed. 2014); John F. Wasik, *Sites To Manage Personal Wealth Gaining Ground*, N.Y. TIMES, Feb. 11, 2014, at F10.

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”).

44. *Data: United States GDP at Market Prices (current US\$)*, WORLD BANK, <http://data.worldbank.org/country/united-states> (last visited Feb. 27, 2015).

times of distress.<sup>45</sup> Eighty-one percent of the global trade financing is conducted using the American dollar.<sup>46</sup> Because of its importance, our currency is the most counterfeited currency in the world by criminals and rogue states.<sup>47</sup> 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.<sup>48</sup> 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.<sup>49</sup>

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 Infrastructural Investment Bank with numerous international member states to serve as a financial counterweight to the United States.<sup>50</sup> 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."<sup>51</sup> 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.<sup>52</sup>

---

45. ZARATE, *supra* note 1, at 9.

46. BREMMER & KUPCHAN, *supra* note 1, at 9.

47. 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).

48. See ZARATE, *supra* note 1, at 12.

49. 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).

50. See Jane Perlez, *Rush To Join China's New Asian Bank Surprises All, Even the Chinese*, N.Y. TIMES, Apr. 3, 2015, at A5.

51. ZARATE, *supra* note 1, at 413 (quoting Admiral Mike Mullen).

52. 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.<sup>53</sup>

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.<sup>54</sup>

## B. 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.”<sup>55</sup> 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. Systemic Risks

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

---

*worked Century*, FOREIGN AFF., Jan.–Feb. 2009, at 94.

53. See generally PAUL VIGNA & MICHAEL J. CASEY, *THE AGE OF CRYPTOCURRENCY: HOW BITCOIN AND DIGITAL MONEY ARE CHALLENGING THE GLOBAL ECONOMIC ORDER* (2015).

54. See ERIC SCHMIDT & JARED COHEN, *THE NEW DIGITAL AGE: TRANSFORMING NATIONS, BUSINESSES, AND OUR LIVES* 82–89 (2014); ZARATE, *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, *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.”).

55. David E. Sanger et al., *U.S. Plans Attack and Defense in Web Warfare*, N.Y. TIMES, Apr. 28, 2009, at A1 (quoting former Director of National Intelligence Mike McConnell).

56. See Scott, *supra* note 6, at 673 (“Going forward, the central problem for financial regulation . . . is to reduce systemic risk.”).

tion in recent years.<sup>57</sup> “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.<sup>58</sup> 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.<sup>59</sup> In 2008, the failings of Bear Stearns and Lehman Brothers caused catastrophic economic stress at home and abroad.<sup>60</sup> 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.”<sup>61</sup> 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

---

57. See, e.g., CONG. OVERSIGHT PANEL, SPECIAL REPORT ON REGULATORY REFORM: MODERNIZING THE AMERICAN FINANCIAL REGULATORY SYSTEM 15–17 (2009) (reporting on the rise of too-big-to-fail financial institutions); ANDREW ROSS SORKIN, TOO BIG TO FAIL: THE INSIDE STORY OF HOW WALL STREET AND WASHINGTON FOUGHT TO SAVE THE FINANCIAL SYSTEM FROM CRISIS—AND THEMSELVES 538–39 (2009) (discussing the policy challenges presented by “too big to fail” institutions); Tom C. Frost, *The Big Danger with Big Banks*, WALL ST. J. (May 16, 2012), <http://www.wsj.com/articles/SB10001424052702304371504577406023330005352>.

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) (“[S]ystemic 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.”).

59. FIN. STABILITY BD., 2014 UPDATE OF LIST OF GLOBAL SYSTEMICALLY IMPORTANT BANKS 3 (2014).

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.<sup>62</sup> 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.<sup>63</sup> 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.<sup>64</sup> 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.”<sup>65</sup> 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.<sup>66</sup> 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; Schwarcz, *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); Schwarcz, *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).

64. See ROGER LOWENSTEIN, WHEN GENIUS FAILED: THE RISE AND FALL OF LONG-TERM CAPITAL MANAGEMENT xviii–xx (2000); FRANK PARTNOY, INFECTIOUS GREED: HOW DECEIT AND RISK CORRUPTED THE FINANCIAL MARKETS 261 (2003).

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. Schwarcz, *Regulating Complexity in Financial Markets*, 87 WASH. U. L. REV. 211, 215 (2009) (“[S]uccessful 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.<sup>67</sup> 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.<sup>68</sup> Yet, because of its important connective role in today's financial network, its proper function is crucial to the system's linked stability.<sup>69</sup> 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, Depository Trust & Clearing Corporation, which clears trillions of dollars in transactions daily, could cause significant economic and psychological damage to our national welfare.<sup>70</sup> 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.<sup>71</sup>

Third, in terms of speed, there exists the systemic risk of "too fast to save."<sup>72</sup> Transactions in the modern financial infrastructure occur at velocities measured in the milliseconds.<sup>73</sup> Billions of dollars move through cables and spectra across seas and states in fractions of a second.<sup>74</sup> While these astounding velocities can be beneficial in terms of efficiencies, they also in-

---

larity . . .").

67. See Nathaniel Popper & Neil Gough, *Bloomberg Data Crash Puts Market in Turmoil*, N.Y. TIMES, Apr. 18, 2015, at B1.

68. *Id.*

69. *Id.*

70. See DEPOSITORY TR. & CLEARING CORP., *SHORTENING THE SETTLEMENT CYCLE: MITIGATING SYSTEMIC RISK AND PROTECTING THE INTEGRITY OF THE U.S. FINANCIAL SYSTEM* (2014).

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.

74. Concept Release on Equity Market Structure, 75 Fed. Reg. 3594, 3610 (proposed Jan. 21, 2010) (acknowledging the accelerating speed of modern financial markets); PATTERSON, *supra* note 34, at 46; A.D. Wissner-Gross & C.E. Freer, *Relativistic Statistical Arbitrage*, 82 PHYSICAL REV. E 056104 (2010) (studying arbitrage opportunities for trading near the speed of light); Graham Bowley, *The New Speed of Money*, N.Y. TIMES, Jan. 2, 2011, at BU1 ("Almost each week, it seems, one exchange or another claims a new record: Nasdaq, for example, says its time for an average order 'round trip' is 98 microseconds—a mind-numbing speed equal to 98 millionths of a second."); Quentin Hardy, *Testing a New Class of Speedy Computer*, N.Y. TIMES, Mar. 22, 2013, at B1; Matthew Philips, *Trading at the Speed of Light*, BLOOMBERG BUSINESSWEEK, Apr. 2, 2012, at 46.

crease the risk of error, volatility, and market misconduct before anyone can intervene to prevent the damage.<sup>75</sup> 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.<sup>76</sup> 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.<sup>77</sup> 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.<sup>78</sup> In less than thirty minutes, approximately \$1 trillion in market value vanished

---

75. See FRANK PARTNOY, WAIT: THE ART AND SCIENCE OF DELAY 43 (2012) (“[O]ther studies show that during periods of high uncertainty . . . high frequency trading is associated with increased volatility and sudden, abrupt swings in the prices of stock.”); CHARLES PERROW, NORMAL ACCIDENTS: LIVING WITH HIGH-RISK TECHNOLOGIES 71 (1999) (discussing the tendency for failures or “accidents” to compound upon one another); Andrew G. Haldane, Exec. Dir. Fin. Stability, Bank of Eng., Speech at the International Economic Association Sixteenth World Congress: The Race to Zero (July 8, 2011) (transcript available at <http://www.bankofengland.co.uk/archive/Documents/historicpubs/news/2011/068.pdf>); see also Fabozzi et al., *supra* note 39, at 29 (discussing how emphasis on speed and technology fragments the financial industry); Floyd Norris, *In Markets’ Tuned-up Machinery, Stubborn Ghosts Remain*, N.Y. TIMES, Aug. 23, 2013, at B1; Matthew Baron et al., *The Trading Profits of High Frequency Traders* (Nov. 2012) (unpublished manuscript), [http://conference.nber.org/confer/2012/MMf12/Baron\\_Brogaard\\_Kirilenko.pdf](http://conference.nber.org/confer/2012/MMf12/Baron_Brogaard_Kirilenko.pdf) (finding that high-frequency traders profit at the expense of ordinary investors).

76. See Concept Release on Equity Market Structure, 75 Fed. Reg. at 3611 (“[M]any proprietary firms potentially could engage in similar or connected trading strategies that, if such strategies generated significant losses at the same time, could cause many proprietary firms to become financially distressed and lead to large fluctuations in market prices.”); Bernard S. Donefer, *Algos Gone Wild: Risk in the World of Automated Trading Strategies*, 5 J. TRADING 31, 32 (2010); Geoffrey P. Miller & Gerald Rosenfeld, *Intellectual Hazard: How Conceptual Biases in Complex Organizations Contributed to the Crisis of 2008*, 33 HARV. J.L. & PUB. POL’Y 807, 810 (2010).

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, *Market Swings Are Becoming New Standard*, N.Y. TIMES, Sept. 12, 2011, at A1.

78. See U.S. COMMODITY FUTURES TRADING COMM’N & U.S. SEC. & EXCH. COMM’N, FINDINGS REGARDING THE MARKET EVENTS OF MAY 6, 2010 1–6 (2010); Graham Bowley, *Lone Sale of \$4.1 Billion in Contracts Led to “Flash Crash” in May*, N.Y. TIMES, Oct. 2, 2010, at B1; see also Nathaniel Popper, *Trader’s Arrest Raises Concern About Market Rigging*, N.Y. TIMES, Apr. 23, 2010, at B1 (discussing how the trading strategy known as spoofing contributed to the flash crash).

from the U.S. stock market.<sup>79</sup> 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.<sup>80</sup>

## 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.<sup>81</sup> The Internet's ubiquity means that any computer that is capable of being connected to the Internet is vulnerable to attack and malice.<sup>82</sup> 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."<sup>83</sup> Many serious crimes and attacks against American corporations now involve computers as the weapons of choice and cyberspace as the preferred setting.<sup>84</sup> For many companies, software codes, intellectual property, and technological infrastructure represent some

---

79. Haldane, *supra* note 75, at 1.

80. See Michael Riley & Ashlee Vance, *The Code War*, BLOOMBERG BUSINESSWEEK, July 25, 2011, at 50.

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.

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.").

83. Mike McConnell, *To Win the Cyber-War, Look to the Cold War*, WASH. POST, Feb. 28, 2010, at B1.

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.<sup>85</sup> 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."<sup>86</sup>

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.<sup>87</sup> This was made alarmingly real by the 2014 hack of Sony Pictures, an American subsidiary of Sony Corporation, by North Korea.<sup>88</sup> A number of similar cyberattacks have been made on American banks and other financial institutions by foreign states and rogue organizations.<sup>89</sup> 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.<sup>90</sup> Due to the amorphous and anonymous nature of cyberattacks—and the reticence of corporate victims to come forward—attribution, prevention, prosecution, and counterstriking can all prove to be difficult.<sup>91</sup>

---

85. See BROWN, *supra* note 33, at 49 (discussing the urgent need for black-box 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 casualties."); Seabrook, *supra* note 13, at 65 ("A large part of the nation's financial infrastructure is under siege [from cyberattacks].").

88. See Michael Cieply & Brooks Barnes, *Sony Attack, First a Nuisance, Swiftly Grew into a Firestorm*, N.Y. TIMES, Dec. 31, 2014, at A1; David E. Sanger & Martin Fackler, *Tracking the Cyberattack on Sony to North Koreans*, N.Y. TIMES, Jan. 19, 2015, at A1.

89. See *infra* notes 96–103.

90. See, e.g., JUNIPER RESEARCH, CYBERCRIME AND THE INTERNET OF THREATS (2015), <http://106.186.118.91/201504/Cybercrime-and-the-Internet-of-Threats.pdf> (estimating that cybercrime costs would be around \$2 trillion by 2019); Nicole Perlroth & Elizabeth A. Harris, *Cyberattack Insurance a Challenge for Business*, N.Y. TIMES, June 9, 2014, at B1.

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.<sup>92</sup> 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.<sup>93</sup> 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-

---

53 (2011) (describing challenges in creating a cybersecurity defense system); Sarah Gordon & Richard Ford, *On the Definition and Classification of Cybercrime*, 2 J. COMPUTER VIROLOGY 13, 13 (2006) (“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); Lynne D. Roberts, *Cyber Identity Theft*, in HANDBOOK OF RESEARCH ON TECHNOETHICS VOL. II 542 (Rocci Luppacini & Rebecca Adell eds., 2009) (acknowledging difficulties in tracing the origins of cyberattacks); Michael Joseph Gross, *Enter the Cyber-Dragon*, VANITY FAIR, Sept. 2011, 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.”); Christopher M. Matthews, *Cybertheft Victims Itchy To Retaliate*, WALL ST. J., June 3, 2013, at B6; Chris Strohm et al., *Cyber Attack? What Cyber Attack?*, BLOOMBERG BUSINESSWEEK, Apr. 15, 2013, at 40 (reporting on the reluctance of companies to disclose cyber attacks).

92. See Caterpillar, Inc., Annual Report (Form 10-K), at 9–11 (Feb. 18, 2014).

93. See The Goldman Sachs Grp., Inc., Annual Report (Form 10-K), at 1 (Feb. 28, 2014).

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.<sup>94</sup> 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.<sup>95</sup>

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.<sup>96</sup> In 2012, large, coordinated attacks, some attributable to Iran, dubbed “Operation High Roller,” targeted American and international financial institutions.<sup>97</sup> 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.<sup>98</sup> In 2014, it was revealed that Russian

---

94. See SEC v. Dorozhko, 574 F.3d 42, 44–45 (2d Cir. 2009) (involving hackers who traded on illicitly-acquired, material, nonpublic information); DEPT OF DEF., THE DEPARTMENT OF DEFENSE CYBER STRATEGY 9 (2015) (“Criminal actors pose a considerable threat in cyberspace, particularly to financial institutions, and ideological groups often use hackers to further their political objectives.”); BOWDEN, *supra* note 91, at 48 (“Today the most serious computer predators are funded by rich criminal syndicates and even nation-states, and their goals are far more ambitious.”); INTELLIGENCE & NAT’L SEC. ALL., CYBER INTELLIGENCE: SETTING THE LANDSCAPE FOR AN EMERGING DISCIPLINE 7–9 (2011); SCOTT PATTERSON, THE QUANTS: HOW A NEW BREED OF MATH WHIZZES CONQUERED WALL STREET AND NEARLY DESTROYED IT 107–16 (2010) (discussing the theft of trade secrets from hedge funds); Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT’L L. 207, 232 (2002) (alluding to the difficulties of identifying a wide cast of potential cyber attackers); Michael Joseph Gross, *Silent War*, VANITY FAIR, July 2013, at 98; Nicole Perlroth, *Hunting for Syrian Hackers’ Chain of Command*, N.Y. TIMES, May 18, 2013, at B1 (reporting on the difficulties of tracing hackers); Nathaniel Popper, *Wall Street’s Exposure to Hacking Laid Bare*, N.Y. TIMES, July 26, 2013, at B1.

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.

96. See Nelson D. Schwartz, *Facing a New Type of Threat from WikiLeaks, a Bank Plays Defense*, N.Y. TIMES, Jan. 3, 2011, at B1.

97. See DAVE MARCUS & RYAN SHERSTOBITOFF, MCAFEE & GUARDIAN ANALYTICS, DISSECTING OPERATION HIGH ROLLER 3–7 (2012); Nicole Perlroth, *Attacks on 6 Banks Frustrate Customers*, N.Y. TIMES, Oct. 1, 2012, at B1; Nicole Perlroth & Quentin Hardy, *Bank Hacks Were Work of Iranians, Officials Say*, N.Y. TIMES, Jan. 9, 2013, at B1.

98. See Amy Chozick & Nicole Perlroth, *Twitter Speaks, Markets Listen, and Fears Rise*, N.Y. TIMES, Apr. 29, 2013, 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.<sup>99</sup> 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.<sup>100</sup> In 2015, it was revealed that an international cyber gang systemically stole millions of dollars from over one hundred institutions around the world.<sup>101</sup> Later that year, an international syndicate of traders and hackers were charged with operating a massive insider trading enterprise.<sup>102</sup> Furthermore, in recent years, China has been privately suspected and publicly accused of serious cybercrimes against American interests.<sup>103</sup> 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.<sup>104</sup>

In addition to an expanding cast of external adversaries, financial institutions must also guard against potential internal adversaries.<sup>105</sup> Rogue employees or contractors with author-

---

99. See FIREEYE, APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS? 3–6 (2014); Michael Riley, *How Russian Hackers Stole the NASDAQ*, BLOOMBERG BUSINESSWEEK, July 20, 2014, at 40.

100. Nicole Perlroth, *Web Thieves Using Lingo of Wall St.*, N.Y. TIMES, Dec. 2, 2014, at B1; see VENERIK ET AL., *supra* note 84, at 3–4.

101. David E. Sanger & Nicole Perlroth, *Bank Hackers Steal Millions Via Malware*, N.Y. TIMES, Feb. 15, 2015, at A1.

102. See Sealed Indictment, *United States v. Shalon et al.*, 15 Crim. 333 (S.D.N.Y. Oct. 22, 2015); Sealed Indictment, *United States v. Murgio*, 15 Crim. 769 (S.D.N.Y. Nov. 10, 2015); Matthew Goldstein & Alexandra Stevenson, *Rogue Traders, Brazen Hackers and a Wave of Arrests*, N.Y. TIMES, Aug. 12, 2015, at B1.

103. See CHINA AND CYBERSECURITY: ESPIONAGE, STRATEGY, AND POLITICS IN THE DIGITAL DOMAIN (Jon R. Lindsay et al. eds., 2015); DENNIS F. POINDEXTER, THE CHINESE INFORMATION WAR: ESPIONAGE, CYBERWAR, COMMUNICATIONS CONTROL AND RELATED THREATS TO UNITED STATES INTERESTS 83–112 (2013); Barboza & Drew, *supra* note 85; Julie Hirschfeld Davis, *Hacking Exposed 21 Million in U.S., Government Says*, N.Y. TIMES, July 10, 2015, at A1; David E. Sanger et al., *China's Army Seen as Tied to Hacking Against U.S.*, N.Y. TIMES, Feb. 19, 2013, at A1; David E. Sanger & Mark Landler, *U.S. and China Will Hold Talks About Hacking*, N.Y. TIMES, June 2, 2013, at A1.

104. Press Release, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), <http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>.

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.<sup>106</sup> 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.<sup>107</sup> 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.<sup>108</sup> Similarly, a rogue programmer or banker with access to critical infrastructure or operational software can cause havoc for the financial system.<sup>109</sup> 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.<sup>110</sup>

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.<sup>111</sup> Venerable American corporations like General Electric had difficulties funding day-to-day operations.<sup>112</sup> McDonald's

---

ble to prevent those authorized to access data from misusing it . . .”).

106. See, e.g., Steven R. Chabinsky, *Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line*, 4 J. NAT'L SECURITY L. & POL'Y 27, 34 (2010); Robin Sidel, *Banks Battle Staffers' Vulnerability to Hacks*, WALL ST. J. (Dec. 20, 2015), <http://www.wsj.com/articles/the-weakest-link-in-banks-fight-against-hackers-1450607401>.

107. See DAVID WISE, *SPY: THE INSIDE STORY OF HOW THE FBI'S ROBERT HANSEN BETRAYED AMERICA* 7–8 (2002).

108. See GLENN GREENWALD, *NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE* 2 (2014).

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).

110. See Nathaniel Popper, *Breach Puts Morgan Data up for Sale*, N.Y. TIMES, Jan. 6, 2015, at B1.

111. See SORKIN, *supra* note 57, at 417; Hui Tong & Shang-Jin Wei, *The Misfortune of Nonfinancial Firms in a Financial Crisis*, in MEASURING WEALTH AND FINANCIAL INTERMEDIATION AND THEIR LINKS TO THE REAL ECONOMY 349–51 (Charles R. Hulten & Marshall B. Reinsdorf eds., 2015).

112. See SORKIN, *supra* note 57, at 417.

franchisees struggled to get loans to make payroll.<sup>113</sup> General Motors went into bankruptcy.<sup>114</sup> And millions of Americans lost their homes, their jobs, and their peace of mind.<sup>115</sup> 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.<sup>116</sup> 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.<sup>117</sup> Ancient Greek and Roman empires deployed financial and economic tactics to decimate their adversaries.<sup>118</sup> As a young nation, the

---

113. *Id.*

114. See ALEX TAYLOR III, *SIXTY TO ZERO: AN INSIDE LOOK AT THE COLLAPSE OF GENERAL MOTORS—AND THE DETROIT AUTO INDUSTRY 1* (2010).

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>.

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.”).

117. See GARY CLYDE HUFBAUER ET AL., *ECONOMIC SANCTIONS RECONSIDERED 9–17* (2009) (providing a historical overview of economic sanctions).

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.<sup>119</sup> 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.<sup>120</sup> 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.<sup>121</sup> Additionally, the G7 nations, through their Financial Action Task Force, also adopted several recommendations against terrorist financing following September 11, 2001.<sup>122</sup> 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.<sup>123</sup> 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-

---

had refused to join the Athenian-led Delian League during the Peloponnesian War.”); ZARATE, *supra* note 1, at 3 (“The Greek city-states, the Roman Empire, and even the barbarians used sieges and economic deprivation to weaken their enemies.”).

119. Embargo Act of 1807, 2 Stat. 451 (1807) (repealed 1809).

120. See Geoffrey Warner, *The Geopolitics and the Cold War*, in THE OXFORD HANDBOOK OF THE COLD WAR 67, 80 (Richard H. Immerman & Petra Goedde eds., 2013).

121. See International Convention for the Suppression of the Financing of Terrorism, Dec. 9, 1999, 2178 U.N.T.S. 38349; S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001).

122. FIN. ACTION TASK FORCE, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM AND PROLIFERATION: THE FATF RECOMMENDATIONS (2013).

123. See U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 116, at 14 (“To move assets, terrorists use mechanisms that enable them to conceal or launder their assets through nontransparent trade or financial transactions such as charities, informal banking systems, bulk cash, and commodities such as precious stones and metals.”); MARTIN A. WEISS, CONG. RESEARCH SERV., RS21902, TERRORIST FINANCING: THE 9/11 COMMISSION RECOMMENDATION 2 (2004) (“Terrorist organizations are increasingly relying on informal methods of money transfer, and regional cells have begun independently generating funds through criminal activity.”); MICHAEL G. FINDLEY ET AL., GLOBAL SHELL GAMES: EXPERIMENTS IN TRANSNATIONAL RELATIONS, CRIME, AND TERRORISM 1–10 (2014); Baradaran et al., *supra* note 1, at 482; J.W. Verret, *Terrorism Finance, Business Associations, and the “Incorporation Transparency Act,”* 70 LA. L. REV. 857, 857–62 (2010) (discussing the post-9/11 terrorism financing methodology); see also Richard Gordon, Response, *A Tale of Two Studies: The Real Story of Terrorism Finance*, 162 U. PA. L. REV. ONLINE 269 (2014), <http://www.pennlawreview.com/online/162-U-Pa-L-Rev-Online-269.pdf>.

portant role in the financial theater of war. Chinese military officials have openly discussed using financial warfare in international conflicts.<sup>124</sup> The United States, as the lone financial superpower in the world, has creatively and effectively used many analog financial weapons against its adversaries.<sup>125</sup> 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.<sup>126</sup> 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.<sup>127</sup> 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.<sup>128</sup> 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.<sup>129</sup> Economic sanctions can include policies like asset freezes, import tariffs, trade barriers, travel restrictions, and embargoes.<sup>130</sup>

---

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.*

128. See Nina J. Crimm, *High Alert: The Government’s War on the Financing of Terrorism and Its Implications for Donors, Domestic Charitable Organizations, and Global Philanthropy*, 45 WM. & MARY L. REV. 1341, 1354 (2004) (“A powerful weapon in the U.S. government’s financial war on terrorism is the use of economic sanctions against terrorists, terrorist groups, and their private sponsors.”); Orde F. Kittrie, *New Sanctions for a New Century: Treasury’s Innovative Use of Financial Sanctions*, 30 U. PA. J. INT’L L. 789, 789 (2009); Lowrey, *supra* note 15, at B1, B5 (“Over the last decade, as sanctions have become vastly more sophisticated, the Obama administration has deployed them more and more often.”).

129. See BRENDAN TAYLOR, SANCTIONS AS GRAND STRATEGY 31 (2010).

130. See Jimmy Gurulé, *The Demise of the U.N. Economic Sanctions Regime To Deprive Terrorists of Funding*, 41 CASE W. RES. J. INT’L L. 19, 20–28 (2009) (explaining the evolution of economic sanctions following September 11, 2001); Nikos Passas, *Combating Terrorist Financing: General Report of the Cleveland Preparatory Colloquium*, 41 CASE W. RES. J. INT’L L. 243, 250–55

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.<sup>131</sup> 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.<sup>132</sup> 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.<sup>133</sup> 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.<sup>134</sup>

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.<sup>135</sup> Anti-money laundering regulations have placed financial institutions at the frontlines of financial warfare.<sup>136</sup> 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.

131. See Keith Bradsher, *China Said To Widen Its Embargo of Minerals*, N.Y. TIMES, Oct. 20, 2010, at B1.

132. See OFFICE OF FOREIGN ASSETS CONTROL, DEP'T. OF TREASURY, SPECIALLY DESIGNATED NATIONALS AND BLOCKED PERSONS LIST (2015); Lowrey, *supra* note 15, at B1.

133. Peter Baker, *Obama Signals Support for New U.S. Sanctions To Pressure Russian Economy*, N.Y. TIMES, Dec. 17, 2014, at A14.

134. *Joint Comprehensive Plan of Action*, WASH. POST (July 14, 2015), <http://apps.washingtonpost.com/g/documents/world/full-text-of-the-iran-nuclear-deal/1651>.

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 . . .”).

136. See Richard K. Gordon, *Trysts or Terrorists? Financial Institutions and the Search for Bad Guys*, 43 WAKE FOREST L. REV. 699, 702–05 (2008).

ment authorities or they could be subject to criminal prosecution.<sup>137</sup> 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.<sup>138</sup> Additionally, post-September 11th, many nations joined forces to help prevent the flow of funds to al Qaeda through new anti-money laundering regulations.<sup>139</sup> 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.<sup>140</sup> 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.<sup>141</sup> 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.<sup>142</sup> 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.<sup>143</sup> 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.<sup>144</sup> Because money is so critical to its

---

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).

138. USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

139. See International Convention for the Suppression of the Financing of Terrorism, *supra* note 121; S.C. Res. 1373, *supra* note 121.

140. See ZARATE, *supra* note 1, at 49–59.

141. *Id.* at ix.

142. Lowrey, *supra* note 15.

143. See JESSICA STERN & J. M. BERGER, ISIS: THE STATE OF TERROR 46 (2015); Rod Nordland, *Iraq Insurgents Reaping Wealth as They Advance*, N.Y. TIMES, June 21, 2014, at A1; David S. Cohen, Remarks of Under Secretary for Terrorism and Financial Intelligence at the Carnegie Endowment for International Peace: Attacking ISIL's Financial Foundation (Oct. 23, 2014), <https://www.treasury.gov/press-center/press-releases/Pages/jl2672.aspx>.

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.<sup>145</sup> In a financial system that revolves around the United States, American financial weaponry is far-reaching and can enlist foreign financial institutions for assistance.<sup>146</sup> 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.<sup>147</sup> 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.<sup>148</sup> 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.”<sup>149</sup> More recent-

---

2015, at A1.

145. See P. EDWARD HALEY, STRATEGIES OF DOMINANCE: THE MISDIRECTION OF U.S. FOREIGN POLICY 5 (2006) (“American primacy gave the United States unprecedented freedom of action and brought coercive diplomacy and economic sanctions into the paradigm with much greater frequency . . . .”); ZARATE, *supra* note 1, at 2–5.

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.”).

147. See 18 U.S.C. § 2339B (2012) (“[T]he term ‘terrorist organization’ means an organization designated as a terrorist organization under section 219 of the Immigration and Nationality Act.”); U.S. DEPT OF THE TREASURY, PROTECTING CHARITABLE GIVING 1 (2010).

148. See Juan C. Zarate, *Harnessing the Financial Furies: Smart Financial Power and National Security*, WASH. Q., Oct. 2009, at 43.

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.<sup>150</sup> 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.<sup>151</sup>

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.<sup>152</sup> 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.<sup>153</sup>

#### 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.<sup>154</sup> America's heavy financial and military reliance on high-tech informational networks render it particularly vulnerable to cyber weapons.<sup>155</sup> The volume and

---

150. See Ben Protess, *German Bank To Pay \$1.5 Billion in U.S. Case*, N.Y. TIMES, Mar. 13, 2015, at B1.

151. See ZARATE, *supra* note 1, at 24 (highlighting the isolating power of banking restrictions); Oona Hathaway & Scott Shapiro, *Outcasting: Enforcement in Domestic and International Law*, 121 YALE L.J. 251, 258 (2001) (describing the exclusionary effect of law as "outcasting").

152. See ROTH ET AL., *supra* note 2, at 27; FIN. ACTION TASK FORCE, *supra* note 3, at 27 ("Even the best efforts of authorities may fail to prevent specific attacks. Nevertheless, when funds available to terrorists are constrained, their overall capabilities decline, limiting their reach and effect.").

153. See Julie Hirschfeld Davis, *Following the ISIS Money*, N.Y. TIMES, Oct. 22, 2014, at B1.

154. See HARRIS, *supra* note 7, at 69–75; Hollis, *supra* note 7, at 1035 ("[Computer network attacks] for example, provides a new weapon that can be deployed instantaneously and surreptitiously thousands of miles away from its target."); Barton Gellman, *Cyber Attacks by al Qaeda Feared: Terrorists at Threshold of Using Internet As Tool of Bloodshed, Experts Say*, WASH. POST, June 27, 2002, at A1; David E. Sanger, *Document Reveals Growth of Cyberwarfare Between the U.S. and Iran*, N.Y. TIMES, Feb. 23, 2015, at A5.

155. See DEP'T OF DEF., *supra* note 94, at 2 ("A disruptive, manipulative, or

varieties of cyberattacks on financial institutions, like all cyberattacks, increase annually.<sup>156</sup> 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.<sup>157</sup> 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.<sup>158</sup> 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.<sup>159</sup>

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.<sup>160</sup> A 2015 Pentagon report found "significant vulnerabilities on nearly every" weapons program under its control.<sup>161</sup> 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).

157. See Mark Landler & John Markoff, *After Computer Siege in Estonia, War Fears Turn to Cyberspace*, N.Y. TIMES, May 29, 2007, at A1.

158. See Barton Gellman & Ellen Nakashima, "Black Budget" Details a War in Cyberspace, WASH. POST, Aug. 31, 2013, at A1; see also Michael Riley, *How the U.S. Government Hacks the World*, BLOOMBERG BUSINESSWEEK, May 27, 2013, at 35-37.

159. See Margaret Coker & Paul Sonne, *Ukraine: Cyberwar's Hottest Front*, WALL ST. J. (Nov. 9, 2015), <http://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671>.

160. Ellen Nakashima, *Pentagon Creates Teams To Launch Cyberattacks as Threat Grows*, WASH. POST (Mar. 12, 2013), [http://articles.washingtonpost.com/2013-03-12/world/37645469\\_1\\_new-teams-national-security-threat-attacks](http://articles.washingtonpost.com/2013-03-12/world/37645469_1_new-teams-national-security-threat-attacks).

161. DEP'T OF DEF. OFFICE OF THE DIRECTOR, OPERATIONAL TEST AND

“29 countries now have formal military or intelligence units dedicated to offensive cyberefforts.”<sup>162</sup> 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.<sup>163</sup> In 2013 alone, it has been reported that “the average American company fielded a total of 16,856 attacks” from cyber weapons.<sup>164</sup> 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.<sup>165</sup> 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.<sup>166</sup> 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.<sup>167</sup> 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.<sup>168</sup> A year later, major banks were again subjected to another round of persistent DDoS attacks,

---

EVALUATION, FY 2014 ANNUAL REPORT 336 (2015) [hereinafter ODOTE].

162. Jennifer Valentino-Devries & Danny Yadron, *Cataloging the World's Cyberforces*, WALL ST. J. (Oct. 11, 2015), <http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710>.

163. Matthew Goldstein, *Firms Wary of Breaches by Hackers, Not Terrorists*, N.Y. TIMES, Feb. 4, 2015, at B8.

164. Lev Grossman, *The Code War*, TIME MAG., July 21, 2014, at 20.

165. Exec. Order No. 13,694, 80 Fed. Reg. 18,077 (Apr. 2, 2015), <https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m>.

166. See Hathaway et al., *supra* note 5, at 837.

167. See ENEKEN TIKK ET AL., NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 66–90 (2010).

168. See, e.g., Perloth, *supra* note 97.

but this time from the nation-state of Iran.<sup>169</sup> 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.<sup>170</sup> 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.<sup>171</sup> 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.<sup>172</sup> 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.<sup>173</sup> 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.<sup>174</sup> 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.

170. Nicole Perlroth, *Chinese Tool Is Suspected in Web Attack*, N.Y. TIMES, Apr. 11, 2015, at B1.

171. See MARTIN C. LIBICKI, CTR. FOR ADVANCED COMMAND CONCEPTS AND TECH., WHAT IS INFORMATION WARFARE? 77 (1995) (describing a semantic attack); Hollis, *supra* note 7, at 1042; Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SEC. L. & POL. 63, 67 (2010) (discussing the effects of cyberattacks on data integrity and authenticity).

172. FIN. INDUS. REGULATORY AUTH., *supra* note 156, at 4.

173. Nicole Perlroth, *Report Says Cyberattacks Originated Inside Iran*, N.Y. TIMES, Dec. 3, 2014, at A14.

174. See Nicole Perlroth, *5 U.S. Banks Hit in Attack by Hackers*, N.Y. TIMES, Aug. 28, 2014, at B1.

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.<sup>175</sup>

Third, in addition to DDoS attacks and data manipulation hacks, destructive intrusion attacks are cyber weapons that are used to destroy critical financial infrastructure.<sup>176</sup> 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.<sup>177</sup> 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.<sup>178</sup> Stuxnet destroyed the centrifuges in the nuclear facility by clandestinely reprogramming them to overwork until destruction.<sup>179</sup> 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.”<sup>180</sup> More recently, in 2015,

---

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.

176. See Nicole Perlroth & David E. Sanger, *Cyberattacks Seem Meant To Destroy, Not Just Disrupt*, N.Y. TIMES, Mar. 29, 2013, at B1; Seabrook, *supra* note 13; Sec’y Jacob J. Lew, U.S. Dep’t of the Treasury, Remarks at the 2014 Delivering Alpha Conference (July 16, 2014).

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.”).

178. See William J. Broad et al., *Israeli Tests Called Crucial in Iran Nuclear Setback*, N.Y. TIMES, Jan. 16, 2011, at A1; see also KIM ZETTER, *COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD’S FIRST DIGITAL WEAPON* 52–70 (2014).

179. Broad et al., *supra* note 178.

180. Andrew E. Kramer & Nicole Perlroth, *Expert Issues a Cyberwar Warning*, N.Y. TIMES, June 3, 2012, at B1.

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.<sup>181</sup> In 2015, it was also reported that Russian hackers had breached Pentagon and White House computer systems, including some of President Obama’s emails.<sup>182</sup> 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.”<sup>183</sup> 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.<sup>184</sup> 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.<sup>185</sup>

Cyberattacks can be particularly challenging to defend against, although public and private actors have made significant strides in improving cybersecurity in recent years.<sup>186</sup> Recognizing the seriousness of cyber weapons against the financial system and other American interests,<sup>187</sup> the federal government has responded to this emerging threat with more aggressive and strategic cyber-defense and cyber weapons programs in re-

---

181. Nicole Perlroth & David E. Sanger, *U.S. Embedded Spyware, Report Says*, N.Y. TIMES, Feb. 17, 2015, at B1.

182. Michael S. Schmidt & David E. Sanger, *Russian Hackers Read Obama’s Unclassified Emails, Officials Say*, N.Y. TIMES, Apr. 26, 2015, at A1.

183. Davis, *supra* note 103.

184. See TED KOPPEL, LIGHTS OUT: A CYBERATTACK, A NATION UNPREPARED, SURVIVING THE AFTERMATH 63 (2015).

185. Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack*, N.Y. TIMES, Oct. 12, 2012, at A1.

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.<sup>188</sup> In 2012 alone, the Air Force spent about \$4 billion on its cyber programs,<sup>189</sup> and the Labor Department, in response to cyber threats, improved the computer security of its valuable economic data.<sup>190</sup> In 2013, it was revealed that President Obama possessed broad powers relating to cyberstrikes against our enemies.<sup>191</sup> 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.<sup>192</sup> 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.<sup>193</sup> That same year, the Department of Defense also released a comprehensive white paper on its cyber strategy.<sup>194</sup> In 2016, the White House announced a Cybersecurity National Action Plan intended to initiate near term and long term actions towards enhancing cybersecurity.<sup>195</sup> 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. *Cf.* 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 “[o]verall the Air Force spends about \$4 billion a year on its cyber programs”).

190. John H. Cushman, Jr., *Guarding the Numbers*, N.Y. TIMES, July 17, 2012, at B1.

191. David E. Sanger & Thom Shanker, *Broad Powers Seen for Obama in Cyberstrikes*, N.Y. TIMES, Feb. 4, 2013, at A1.

192. Exec. Order No. 13636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

193. *Executive Order—Promoting Private Sector Cybersecurity Information Sharing*, WHITE HOUSE (Feb. 13, 2015), <http://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>; see also House Amendment #1 to the Senate Amendment to H.R. 2029, 114th Cong. (2015) (amending the Military Construction and Veterans Affairs and Related Agencies Appropriations Act); Damian Paletta & Danny Yadron, *Administration Creates Office To Battle Hacking*, WALL ST. J., Feb 11, 2015, at A4.

194. DEP'T OF DEF., *supra* note 94.

195. WHITE HOUSE, FACT SHEET: NATIONAL CYBERSECURITY ACTION PLAN (Feb. 9, 2016), <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>.

tems and purchase insurance in connection with these attacks.<sup>196</sup> 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.<sup>197</sup>

### 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.”<sup>198</sup> 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.<sup>199</sup> 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.<sup>200</sup> 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.<sup>201</sup> 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 . . .”).

198. MARY L. DUDZIAK, WAR TIME: AN IDEA, ITS HISTORY, ITS CONSEQUENCES 3 (2012) (quoting Cicero).

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.”).

200. See, e.g., Koh, *supra* note 5, at 1772 (“Increasingly, we find ourselves addressing twenty-first-century challenges with twentieth-century laws.”); David Wippman, *The Nine Lives of Article 2(4)*, 16 MINN. J. INT’L L. 387, 388–90 (2007) (arguing that Article 2(4) of the U.N. Charter continues to be influential).

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 Clan-destine 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.”<sup>202</sup> 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.<sup>203</sup>

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.<sup>204</sup> 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.<sup>205</sup> In fact, drafters of the United Nations Charter considered and rejected the view that economic coercion should be a prohibited use of force.<sup>206</sup> The United Nations, furthermore, has long used economic sanctions as one of its governance tools.<sup>207</sup> Additionally, states regu-

---

461–63 (2014) (explaining how terrorist groups threaten conventional war and peacetime standards); Waxman, *supra* note 5, at 424.

202. North Atlantic Treaty, art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

203. See, e.g., INT’L COMM. OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 31–36, 71–73 (2009); Waxman, *supra* note 5, at 422 (“Most economic and diplomatic measures, even if they exact tremendous costs on target states (including significant loss of life) are generally not barred by the U.N. Charter, though some of them may be barred by other legal principles.”).

204. See, e.g., DANIEL W. DREZNER, THE SANCTIONS PARADOX: ECONOMIC STATECRAFT AND INTERNATIONAL RELATIONS 15–17 (1999) (discussing the purpose of economic hostilities in the context of diplomacy); Hathaway et al., *supra* note 5, at 445 (noting problems from applying traditional laws of war to attacks on financial systems); Christina Parajon Skinner, *An International Law Response to Economic Cyber Espionage*, 46 CONN. L. REV. 1165, 1194 (2014) (arguing for the use of international trade law to combat economic cyber espionage).

205. See, e.g., Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKELEY J. INT’L L. 525, 551 (2012) (“Article 2(4) [of the United Nations Charter] did not categorize economic coercion as a prohibited use of force. Nowhere in the Charter is economic coercion prohibited.”).

206. U.N. Conference on Int’l Org., *Amendments of the Brazilian Delegation to the Dumberton Oaks Projects*, U.N. Doc. 2, G/7 (e)(3), at 252–53 (1945).

207. See JEREMY MATAM FARRALL, UNITED NATIONS SANCTIONS AND THE RULE OF LAW 3 (2007) (enumerating various levels of economic sanctions passed by the United Nations).

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.<sup>208</sup> 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.<sup>209</sup>

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.<sup>210</sup> 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.<sup>211</sup> The Russians have hacked into the NASDAQ, and have made covert attempts to destabilize our capital markets.<sup>212</sup> 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.<sup>213</sup> Various non-state actors have also made serious attempts to cause significant damage to our civilian financial institutions.<sup>214</sup>

As cool and cold wars grow warm and hot, these tensions between traditional laws of war and modern financial hostilities will continue to persist.<sup>215</sup> 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.<sup>216</sup> 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.<sup>217</sup> There are no clear strategies for cyberattacks despite the enormous potential financial fallout and physical destruction that can occur from cyberattacks.<sup>218</sup> Numerous basic questions about cyberattacks in the financial realm and beyond continue to lack a wide and

---

213. See, e.g., Perloth & Hardy, *supra* note 97.

214. See, e.g., Schwartz, *supra* note 96.

215. See, e.g., NOAH FELDMAN, COOL WAR: THE FUTURE OF GLOBAL COMPETITION (2014) (describing the cool war between China and the United States).

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 (“[A]pplying 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).

218. See Hollis, *supra* note 7, at 1035; David E. Sanger, *Countering Cyberattacks Without a Playbook*, N.Y. TIMES, Dec. 24, 2014, at A3; Michael Crowley & Josh Gerstein, *No Rules of Cyber War*, POLITICO (Dec. 23, 2014), <http://www.politico.com/story/2014/12/no-rules-of-cyber-war-113785.html>; see also JOE KLEIN, THE NATURAL: THE MISUNDERSTOOD PRESIDENCY OF BILL CLINTON 190 (2002) (“[Following September 11, 2001,] the Treasuries Secretaries Robert Rubin and Lawrence Summers opposed cyber-warfare on grounds that it may threaten the stability of the international financial system.”).

clear consensus among key international stakeholders.<sup>219</sup> 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.<sup>220</sup> 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.<sup>221</sup> Is cyberspace a new extra-sovereign domain given its inherent extra-territorial nature?<sup>222</sup> 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.<sup>223</sup> The United States has defined cyberspace as “the inter-

---

219. See Eichensehr, *supra* note 7, at 320 (discussing how states “disagree about almost everything” relating to cyber issues); Karl Rauscher, *Writing the Rules of Cyberwar*, IEEE SPECTRUM, Dec. 2013, at 30 (advocating for new international conventions on cyberwarfare).

220. See Johnson & Post, *supra* note 7, at 1367 (“Global computer-based communications cut across territorial borders, creating a new realm of human activity and undermining the feasibility—and legitimacy—of laws based on geographic boundaries.”); Lessig, *supra* note 7, at 514–22 (describing various regulatory challenges posed by the amorphous boundaries of cyberspace); May, *supra* note 217, at 6.

221. See JOHN KISH, INTERNATIONAL LAW AND ESPIONAGE 83 (David Turns ed., 1995) (“The general principle of exclusive sovereignty over national territory is firmly established in customary international law. Each State exercises control over its national territory to the exclusion of all other States, and any limitation of this authority is subject to the consent of the territorial State.”); ROBERT K. KNAKE, COUNCIL ON FOREIGN RELATIONS, INTERNET GOVERNANCE IN AN AGE OF CYBER SECURITY 16 (2010) (“Whereas national legal authority is bounded by borders, the Internet is not.”); Kristen E. Eichensehr, *Cyberwar & International Law Zero Step*, 50 TEX. INT’L L.J. 355, 368 (2015) (“[I]nternational law has traditionally operated at the level of sovereign States . . .”).

222. See Goldsmith, *supra* note 7, at 1200–01; Eugene Kontorovich, *The Piracy Analogy: Modern Universal Jurisdiction’s Hollow Foundation*, 45 HARV. INT’L L.J. 183, 190–92 (2004).

223. See, e.g., JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 476 (2008); LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 391 (2006) (“There has been a rich, and sometimes unnecessary, debate about whether indeed cyberspace is a ‘place.’”); Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475, 476 (1998) (“The Internet is not, as many suggest, a separate place removed from our world. Like the telephone, the telegraph, and the smoke signal, the Internet is a medium through which people in real space in one jurisdiction communicate with people in real space in another jurisdiction.”); David G. Post, *Against “Against Cyberanarchy,”* 17 BERKELEY TECH. L.J. 1363, 1366 (2002) (“Communication in cyberspace is not ‘functionally identical’ to communication in real space . . . . Furthermore, the jurisdictional and choice-of-law dilemmas posed by cyberspace activity cannot be adequately resolved by applying the

dependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.<sup>224</sup> 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.<sup>225</sup> Nonetheless, unlike traditional warfare, there remains no clear consensus on this important question relating to sovereignty and jurisdiction.<sup>226</sup> 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.<sup>227</sup> 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.<sup>228</sup>

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.<sup>229</sup> 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?<sup>230</sup> What and how should the law consider a

---

‘settled principles’ and ‘traditional legal tools’ developed for analogous problems in realspace.”).

224. WHITE HOUSE, CYBERSPACE POLICY REVIEW 1 (2009).

225. See DEPT OF DEF. OFFICE OF THE SEC’Y OF DEF., ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE’S REPUBLIC OF CHINA 2013 37 (2013); Eichensehr, *supra* note 7, at 329–30.

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.”).

228. See Duncan B. Hollis, *Re-Thinking the Boundaries of Law in Cyberspace: A Duty To Hack?*, in CYBERWAR, *supra* note 7, at 131; Eric Talbot Jensen, *Future War and the War Powers Resolution*, 29 EMORY INT’L L.J. 499, 537–39 (2015); Anne-Marie Slaughter, *Sovereignty and Power in a Networked World Order*, 40 STAN J. INT’L L. 283, 284–87 (2004); Sanger, *supra* note 218.

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?<sup>231</sup> These questions are already complex for traditional operations, but become even more vexing for cyber operations relating to financial institutions and financial infrastructure.<sup>232</sup> 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.<sup>233</sup> 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.<sup>234</sup> GhostNet gave an outside party complete control and occupation of another party's computer system without detection.<sup>235</sup> 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).

232. See, e.g., *Lowry v. Reagan*, 676 F. Supp. 333, 340 n.53 (D.D.C. 1987); *Libya and War Powers: Hearing Before S. Foreign Relations Comm.*, 112th Cong. 22 (2011) (prepared statement of Hon. Harold Koh, Legal Adviser, U.S. Dep't of State); Allison Arnold, *Cyber “Hostilities” and the War Powers Resolution*, 217 MIL. L. REV. 174, 180–82 (2013).

233. Sanger, *supra* note 218.

234. See INFO. WARFARE MONITOR, TRACKING GHOSTNET: INVESTIGATING A CYBER ESPIONAGE NETWORK 5–22 (2009).

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.<sup>236</sup> However, because GhostNet is a software program likely attributable to China, the rules of engagement are not as clear.<sup>237</sup> 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.<sup>238</sup> 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.<sup>239</sup> As a result of these challenges, to date, there are no widely accepted treaties or norms governing the use of cyber weapons.<sup>240</sup>

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).<sup>241</sup> 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.<sup>242</sup> 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).

238. See Hathaway et al., *supra* note 5, at 826; Hollis, *supra* note 7, at 1045 (opining on the challenges of translating existing rules of conflict into the context of cyberattacks); William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, 89 FOREIGN AFF. 97, 108 ("The cyberthreat does not involve the existential implications ushered in by the nuclear age . . ."); Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, Remarks at the USCYBERCOM Inter-Agency Legal Conference: International Law in Cyberspace (Sept. 18, 2012), in 54 HARV. INT'L L.J. ONLINE, Dec. 13, 2012.

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.

issues.<sup>243</sup> China and Russia, alternatively, generally prefer a sovereignty-oriented model of cyber governance that gives individual states most of the power.<sup>244</sup> 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.<sup>245</sup> 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.<sup>246</sup> For instance, there is no clear, widely accepted agreement on the obligations of states regarding their due diligence duties to prevent cyberattacks on other states that originate within their sovereign territory.<sup>247</sup>

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.<sup>248</sup> 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.<sup>249</sup> 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.

245. See Andrew Jacobs, *China Further Tightens Grip on the Internet*, N.Y. TIMES, Jan. 30, 2015, at A1; Paul Mozur & Jane Perlez, *China Halts New Policy on Tech for Banks*, N.Y. TIMES, Apr. 17, 2015, at B1.

246. See Sanger, *supra* note 218.

247. See Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 YALE L.J. F. 68, 69–70 (2015).

248. See Hathaway et al., *supra* note 5, at 859–77 (providing an overview of a patchwork of international law relating to cyberattacks).

249. See William H. Boothby, *Methods and Means of Cyber Warfare*, 89 INT’L L. STUD. 387 (2013); Eichensehr, *supra* note 7; Jack Goldsmith, *How Cyber Changes the Laws of War*, 24 EUR. J. INT’L L. 129 (2013); Eric Talbot Jensen, *Cyber Attacks: Proportionality and Precautions in Attack*, 89 INT’L L. STUD. 198 (2013); Michael N. Schmitt, *Classification of Cyber Conflict*, 89 INT’L L. STUD. 233 (2013); see also GABRIELLA BLUM, ISLANDS OF AGREEMENTS: MANAGING ENDURING ARMED RIVALRIES 4 (2007) (discussing a theory that highlights coexistence of conflict and cooperation among rival states).

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.<sup>250</sup> 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.<sup>251</sup> That same year, the United Nations also issued a report of recommendations on information and telecommunications security.<sup>252</sup> 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.<sup>253</sup> 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.”<sup>254</sup> 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.<sup>255</sup> And in 2015, the United States and China reached a preliminary agreement concerning broad principles relating to cybersecurity.<sup>256</sup> 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).

251. See Grossman, *supra* note 164, at 23; THE WASSENAAR ARRANGEMENT, <http://www.wassenaar.org> (last updated Jan. 20, 2016).

252. See U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/68/156 (July 16, 2013); see also U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/70/172 (July 22, 2015).

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.<sup>257</sup>

### 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.<sup>258</sup> While non-state adversaries like terrorist organizations have existed for centuries, much of the legal infrastructure remains better suited to address state adversaries.<sup>259</sup> As non-state adversaries continue to play more prominent roles in modern warfare, tensions arise when old doctrines mismatch new realities.<sup>260</sup> Non-state adversaries present spe-

---

operation and the Establishment of an Exchange and Communication Mechanism Between the United States Agency for International Development and the Ministry of Commerce of the People's Republic of China, China-U.S., Sept. 25, 2015, <https://www.usaid.gov/china/mou>; see also *First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes*, U.S. DEP'T OF JUST. (Dec. 2, 2015), <http://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary-outcomes-0>.

257. See, e.g., Ashley Deeks, *The Geography of Cyber Conflict: Through a Glass Darkly*, 89 INT'L L. STUD. 1, 5–10 (2013); Eichensehr, *supra* note 221, at 370–75; Hathaway et al., *supra* note 5, at 856.

258. See Nicolò Bussolati, *The Rise of Non-State Actors in Cyberwarfare*, in CYBERWAR, *supra* note 7, at 103, 102–06; see also Kenneth Anderson, *U.S. Counterterrorism Policy and Superpower Compliance with International Human Rights Norms*, 30 FORDHAM INT'L L.J. 455, 472 (2007) (opining that the war on terror does not meet the requirements of war under traditional legal understandings of the concept); Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 102 (2001) (“International law focuses on states, but the growing power of non-state actors, such as insurgent groups, multinational corporations, transnational criminal organizations, and non-governmental organizations, is a challenge for traditional international law.”); Huntley & Levitz, *supra* note 201, at 482 (noting the debate concerning the applicability of the law of armed conflict to non-state terrorists).

259. See generally MICHAEL BURLEIGH, *BLOOD AND RAGE: A CULTURAL HISTORY OF TERRORISM* (2010); THE HISTORY OF TERRORISM: FROM ANTIQUITY TO AL QAEDA (Gérard Chaliand & Arnaud Blin eds., 2007).

260. See, e.g., Gabriella Blum & Philip B. Heymann, *Law and Policy of Targeted Killing*, 1 HARV. NAT'L SEC. J. 145, 147 (2010) (highlighting legal issues involved with killing alleged terrorists); David Glazier, *Playing by the Rules: Combating al Qaeda Within the Law of War*, 51 WM. & MARY L. REV. 957, 962–63 (2009) (explicating the applicability of law in connection with non-state actors); Katyal & Tribe, *supra* note 5, at 1260 (highlighting the constitutional challenges involved with trying terrorists); Michael Schmitt, *Bellum Americanum: The U.S. View of Twenty-First Century War and Its Possible Im-*

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.<sup>261</sup> For instance, the Hague Conventions of 1899 banned the use of certain poisonous arms in warfare among nations.<sup>262</sup> 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.<sup>263</sup> However, unlike state actors, it is much more difficult to enter into legal agreements about wartime behavior with non-state adversaries.<sup>264</sup> 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.<sup>265</sup> 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,

---

*plications for the Law of Armed Conflict*, 19 MICH. J. INT'L L. 1051, 1073–74 (1998) (“If twenty-first century national security threats are to come from non-state actors, then the law governing the resort to force is bound to evolve in a way that permits an effective defense against them . . .”).

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.”).

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.

263. COUNCIL OF EUR., *EUROPEAN TREATY SERIES: CONVENTION ON CYBERCRIME* (2001).

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.”).

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.”).

“adhering to standards, international standards, strengthens those who do, and isolates and weakens those who don’t.”<sup>266</sup>

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.<sup>267</sup> 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).<sup>268</sup> Non-state adversaries like hackers, terrorists, and lone-wolf combatants are frequently much more difficult to trace and find, let alone hold accountable.<sup>269</sup> 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.<sup>270</sup> 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.<sup>271</sup> In the absence of clear international law and military mechanisms,

---

266. President Barack H. Obama, Nobel Lecture: A Just and Lasting Peace (Dec. 10, 2009), [http://www.nobelprize.org/nobel\\_prizes/peace/laureates/2009/obama-lecture\\_en.html](http://www.nobelprize.org/nobel_prizes/peace/laureates/2009/obama-lecture_en.html).

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).

268. See DAVID A. BALDWIN, *ECONOMIC STATECRAFT* 130–33 (1985) (explaining how states can create accountability mechanisms via economic sanctions); JACK L. GOLDSMITH & ERIC A. POSNER, *THE LIMITS OF INTERNATIONAL LAW* 225–26 (2005) (discussing the motivations and limitations of cooperation among nations); Eichensehr, *supra* note 7, at 370–71; Mary Ellen O’Connell, *Enhancing the Status of Non-State Actors Through a Global War on Terror?*, 43 COLUM. J. TRANSNAT’L L. 435, 445 (2005).

269. See M. Cherif Bassiouni, *The New Wars and the Crisis of Compliance with the Law of Armed Conflict by Non-State Actors*, 98 J. CRIM. L. & CRIMINOLOGY 711, 715 (2008) (“[N]on-state actors have no expectation of accountability for their non-compliance.”); Joseph S. Nye, Jr., *Nuclear Lessons for Cyber Security?*, STRATEGIC STUD. Q., Winter 2011, at 20.

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.<sup>272</sup> 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.<sup>273</sup> 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.<sup>274</sup> As such, if attribution is uncertain, enforcement is frequently unachievable at a just and satisfactory level.<sup>275</sup>

\* \* \*

The world changes swiftly, and the law changes slowly.<sup>276</sup> This Aesopian turtle and hare dynamic leads to tensions when old rules meet new concerns in modern warfare.<sup>277</sup> Innovations at the intersection of modern war and finance exhibit this tense dynamic.<sup>278</sup> 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 . . .”).

273. See *id.*; George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT’L L. 1079, 1174–95 (2000) (discussing the issue of neutral states in cyberwarfare).

274. See Jens David Ohlin, *Cyber Causation*, in CYBERWAR, *supra* note 7, at 37–44; Michael N. Schmitt & Liis Vihul, *Proxy Wars in Cyber Space: The Evolving International Law of Attribution*, 1 FLETCHER SEC. REV., no. 2, at 55 (2014); Jack Goldsmith, *The New Vulnerability*, NEW REPUBLIC, June 24, 2010, at 21, 23.

275. See COMM. ON OFFENSIVE INFO. WARFARE, NAT’L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 252–53 (2009); Marco Roscini, *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations*, in CYBERWAR, *supra* note 7, at 215–17.

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.<sup>279</sup> 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.<sup>280</sup>

#### 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.<sup>281</sup> While many larger legal and political questions concerning financial warfare

---

*tional Money: Regulation in a Global Capital Market*, 65 FORDHAM L. REV. 1855, 1856–57 (1997) (discussing how globalization has increased the burden of capital market regulators to maintain adequate disclosure, antifraud, and anti-manipulation rules); Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 INT'L L. STUD. 99, 114–15 (2002) (“The novelty of a weapon—any weapon—always baffles statesmen and lawyers, many of whom are perplexed by technological innovations. . . . [A]fter a period of gestation, it usually dawns on belligerent parties that there is no insuperable difficulty in applying the general principles and rules of international law to the novel weapon . . . .”); Whitehead, *supra* note 6, at 2–5 (noting the lack of regulatory innovation in response to financial innovation); Julia L. Chen, Note, *Restoring Constitutional Balance: Accommodating the Evolution of War*, 53 B.C. L. REV. 1767, 1788–92 (2012) (discussing how the new methodologies of warfare challenge traditional understandings of war powers).

279. Hathaway et al., *supra* note 5, at 840.

280. 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.”).

281. 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 lawmaking 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.”).

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.<sup>282</sup> 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.<sup>283</sup> 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.<sup>284</sup> Because much of the critical financial infrastructure is owned and operated by private businesses,<sup>285</sup> 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 institutional stability.<sup>286</sup>

A pure market-based approach towards cybersecurity may be inadequate for building better defenses against dynamic threats.<sup>287</sup> 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 Department, Target, J.P. Morgan Chase, and Home Depot all suffered serious cybersecurity breaches.<sup>288</sup> 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 investments are growing in response to increased threats.<sup>289</sup> 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 investments in the near future.<sup>290</sup> 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 encourage more proactive and timely behavior among more private firms.<sup>291</sup>

---

286. See STEWART BAKER ET AL., MCAFEE, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 14 (2009); NY DEP'T OF FIN. SERV., REPORT ON CYBER SECURITY IN THE BANKING SECTOR 11 (May 2014) (highlighting resource constraints and stale software as ongoing challenges for financial cybersecurity); Nicole Perlroth, *Hacked vs. Hackers: Game On*, N.Y. TIMES, Dec. 3, 2014, at F1 (reporting on the lack of urgency regarding cybersecurity).

287. JOEL BRENNER, AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE 239 (2011).

288. See Perlroth, *supra* note 286.

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

290. See JPMorgan Chase & Co., Annual Report (Form 10-K), at 142 (Feb. 24, 2015); JPMorgan Chase & Co., 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 defense capabilities.").

291. Huang et al., *supra* note 289; Jessica Silver-Greenberg & Matthew Goldstein, *After Breach, Push To Close Security Gaps*, N.Y. TIMES, Oct. 22, 2014, at B1; see, e.g., Derek E. Bambauer, *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.<sup>292</sup> 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.<sup>293</sup> 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.<sup>294</sup> 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.<sup>295</sup> If direct, open

---

aging better cybersecurity).

292. See JANE G. GRAVELLE, CONG. RESEARCH SERV., BONUS DEPRECIATION: ECONOMIC AND BUDGETARY ISSUES 4 (2014); GARY GUENTHER, CONG. RESEARCH SERV., SECTION 179 AND BONUS DEPRECIATION EXPENSING ALLOWANCES: CURRENT LAW, LEGISLATIVE PROPOSALS IN THE 113TH CONGRESS, AND ECONOMIC EFFECTS 1 (2014); INTERNAL REVENUE SERV., HOW TO DEPRECIATE PROPERTY 3–24 (2015), <https://www.irs.gov/pub/irs-pdf/p946.pdf>; ERIC ZWICK & JAMES MAHON, DO FINANCIAL FRICTIONS AMPLIFY FISCAL POLICY? EVIDENCE FROM BUSINESS INVESTMENT STIMULUS 39 (Jan. 7, 2014), <http://scholar.harvard.edu/files/zwick/files>; James M. Williamson & John L. Pender, *Economic Stimulus and the Tax Code: The Impact of the Gulf Opportunity Zone*, 1 Pub. Fin. Rev. 3 (2014), <http://pfr.sagepub.com/content/early/2014/12/11/1091142114557724.full.pdf>.

293. *Business Provisions of the American Recovery and Reinvestment Act of 2009*, INTERNAL REVENUE SERV., [https://www.irs.gov/uac/Business-Provisions-of-the-American-Recovery-and-Reinvestment-Act-of-2009-\(ARRA\)](https://www.irs.gov/uac/Business-Provisions-of-the-American-Recovery-and-Reinvestment-Act-of-2009-(ARRA)) (last updated Mar. 19, 2014).

294. See, e.g., Daniel P. Gitterman, *The American Presidency and the Power of the Purchaser*, 43 PRESIDENTIAL STUD. Q. 225, 225–29 (2013) (describing the use of procurement to shape public policy).

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.<sup>296</sup> Private firms like Google and Microsoft already participate in this cyber arms marketplace.<sup>297</sup> 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.<sup>298</sup> 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.<sup>299</sup> 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.<sup>300</sup> 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.<sup>301</sup> 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.<sup>302</sup>

---

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).

301. See Security Requirements for Unclassified Information Resources, 48 C.F.R. § 552.239-71 (2015).

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.<sup>303</sup> It may be necessary for the government to initiate and coordinate some of the desired outcomes.<sup>304</sup> Proper public policy incentives could mitigate some of the collective action problems associated with cybersecurity.<sup>305</sup> 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.<sup>306</sup> 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.<sup>307</sup> 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

---

ed Mar. 7, 2016).

303. See, e.g., Bambauer, *supra* note 7, at 1036 ("Rational vendors will accordingly skimp on security investments, at least at the margins, since they will likely not be able to recover those costs via higher prices that correlate with higher quality.").

304. See, e.g., Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 662–64 (2011) (discussing the need for government regulation to encourage private companies to cooperate with one another to decrease cyber security risk).

305. See Bambauer, *supra* note 7, at 1031 ("[C]ybersecurity suffers from a collective-action problem.").

306. See *Hearing to Receive Testimony on U.S. Strategic Command and U.S. Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2014 and the Future Years Defense Program Before the S. Comm. on Armed Servs.*, 113th Cong. 32 (2013) (statement of Sen. Richard Blumenthal).

307. See, e.g., James A. "Sandy" Winnefeld, Jr. et al., *Cybersecurity's Human Factor: Lessons from the Pentagon*, HARV. BUS. REV., Sept. 2015, at 86, 94 (discussing use of operational tests to enhance cybersecurity).

Communications Integration Center.<sup>308</sup> These tests can help address some of the informational challenges associated with cybersecurity.<sup>309</sup> 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.<sup>310</sup> 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.<sup>311</sup> 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.<sup>312</sup> 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.<sup>313</sup> The Fi-

---

308. See generally *National Cybersecurity and Communications Integration Center*, HOMELAND SEC., <http://www.dhs.gov/national-cybersecurity-communications-integration-center> (last updated Jan. 19, 2016) (describing the role of the National Cybersecurity and Communications Integration Center).

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 238, at 97; Nye, *supra* note 269.

312. See Standards for Safeguarding Customer Information, 16 C.F.R. § 314.3–4 (2015); Office of Compliance Inspections & Examinations, Sec. & Exch. Comm'n, *Cybersecurity Examination Sweep Summary*, 4 NAT'L EXAM PROGRAM RISK ALERT 2 (2015) (“The vast majority of examined firms conduct periodic risk assessments, on a firm-wide basis, to identify cybersecurity threats, vulnerabilities, and potential business consequences.”).

313. Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators, 63 Fed. Reg. 41,804, 41,804–06 (Aug. 5, 1998); *About FS-ISAC*, FIN. SERVS. INFO. SHARING & ANALYSIS CTR., <https://www.fsisac.com/about> (last visited Mar. 7, 2016).

financial Services Modernization Act of 1999 mandates that regulated institutions meet certain benchmarks for protecting the financial information of their customers.<sup>314</sup> Similarly, the Pentagon also runs annual tests on all of its major weapon systems, including assessments for cybersecurity.<sup>315</sup> 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.<sup>316</sup> And in 2015, collectives of private firms created platforms like Soltra and ThreatExchange to share information about cyberthreats.<sup>317</sup>

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.<sup>318</sup> Because that bill did not become law, President Obama signed an executive order focused on improving the cybersecurity of our nation's critical infrastructure.<sup>319</sup> 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.<sup>320</sup> Given the importance of our financial system, efforts to better protect our critical infrastructure from cyberattacks should include our financial infrastructure and its

---

314. See generally 12 U.S.C. § 1811 (2012) (establishing the Federal Deposit Insurance Corporation); 15 U.S.C. § 6801–09 (2012) (mandating protection of customer information); 16 C.F.R. §§ 314.1–314.5 (2002) (regulation effecting the statutory mandate).

315. ODOE, *supra* note 161, at 331–37.

316. See FIN. INDUS. REGULATORY AUTH., *supra* note 156, at 34 (highlighting the importance of information sharing in cybersecurity).

317. Press Release, Soltra, New Soltra Network Offering To Connect and Coordinate Cyber Threat Sharing (Oct. 12, 2015), <https://soltra.com/pdf/Soltra%20Network%20Press%20Release%20101215.pdf>; Threatexchange, FACEBOOK, <https://www.facebook.com/threatexchange/info> (last visited Mar. 7, 2016).

318. Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013).

319. Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (2013).

320. NAT'L INST. OF STANDARDS & TECH., IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY EXECUTIVE ORDER 13636: PRELIMINARY CYBERSECURITY FRAMEWORK 1 (2013).

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.<sup>321</sup> 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.<sup>322</sup> 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.<sup>323</sup> 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.<sup>324</sup> Foreign banking regulators have also implemented similar stress tests for their systemically important financial institutions.<sup>325</sup> These stress tests, while imperfect, can nonetheless provide valuable information for policymakers and tested financial institutions.<sup>326</sup>

---

321. See 12 U.S.C. § 5365(a) (2012) (calling for development of standards to apply to banks with assets in excess of \$50 billion); Supervisory Stress Test Requirements for U.S. Bank Holding Companies with \$50 Billion or More in Total Consolidated Assets and Nonbank Financial Companies Supervised by the Board, 12 C.F.R. § 252.41–47 (2015) (implementing stress tests); DAVID SKEEL, *THE NEW FINANCIAL DEAL: UNDERSTANDING THE DODD-FRANK ACT AND ITS (UNINTENDED) CONSEQUENCES* 77–80 (2011) (noting special requirements for banks with over \$50 billion in assets); Baradaran, *supra* note 6, at 1250–51 (critiquing stress tests).

322. See Baradaran, *supra* note 6, at 1283 (describing stress tests); Robert Weber, *A Theory for Deliberation-Oriented Stress Testing Regulation*, 98 MINN. L. REV. 2236, 2238–39 (2014) (describing what stress tests reveal).

323. Press Release, Fed. Reserve (Mar. 7, 2013) <http://www.federalreserve.gov/newsevents/press/bcreg/20130307a.htm>.

324. See BD. OF GOVERNORS OF THE FED. RESERVE SYS., *DODD-FRANK ACT STRESS TEST 2014: SUPERVISORY STRESS TEST METHODOLOGY AND RESULTS 1* (2014).

325. See, e.g., EUROPEAN BANKING AUTH., *2011 EU-WIDE STRESS TEST AGGREGATE REPORT 2–4* (2011) (reporting results of 2011 stress test); Andrew Haldane, Exec. Dir. for Fin. Stability, Bank of Eng., *Speech at the Marcus-Evans Conference on Stress Testing: Why Banks Failed the Stress Test* (Feb. 13, 2009), <http://www.bankofengland.co.uk/archive/Documents/historicpubs/speeches/2009/speech374.pdf> (describing stress testing in the United Kingdom).

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.<sup>327</sup> 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.<sup>328</sup> 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-

---

ing, 12 C.F.R. pt. 252 app. A(1)(e) (2014) (“[Stress testing is] a valuable supervisory tool that provides a forward-looking assessment of large financial companies’ capital adequacy under hypothetical economic and financial market conditions.”); SENIOR SUPERVISORS GRP., RISK MANAGEMENT LESSONS FROM THE GLOBAL BANKING CRISIS OF 2008 26 (2009) (discussing various problems in connection with capital stress testing); Baradaran, *supra* note 6, at 1250–53 (highlighting shortcomings of financial stress testing); M. Todd Henderson & Frederick Tung, *Pay for Regulator Performance*, 85 S. CAL. L. REV. 1003, 1021–23 (2012) (discussing the failings of banking examiners, including those associated with stress testing).

327. See, e.g., DEP’T OF TREASURY, OFFICE OF INSPECTOR GEN., AUDIT REPORT 4–5 (Sept. 15, 2014), <https://s3.amazonaws.com/s3.documentcloud.org/documents/2178548/oig-report.pdf> (detailing vulnerabilities in the information systems at the Treasury Department).

328. Matthew Goldstein, *Law Firms Are Pressed on Security for Data*, N.Y. TIMES, Mar. 27, 2014, at B1; Huang et al., *supra* note 289; Carter Dougherty, *Banks Dreading Computer Hacks Call for Cyber War Council*, BLOOMBERG BUSINESSWEEK (July 8, 2014 10:40 AM), <http://www.bloomberg.com/news/articles/2014-07-08/banks-dreading-computer-hacks-call-for-cyber-war-council>.

equipped to handle technological stresses and threats from foreign and domestic adversaries.<sup>329</sup>

### 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.<sup>330</sup> 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.<sup>331</sup> 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.<sup>332</sup> 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.<sup>333</sup> 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 DEPT 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 policy-makers to anticipate the complexities surrounding financial warfare.<sup>334</sup>

War games have long been used by militaries, here and abroad, to enhance readiness and national defenses.<sup>335</sup> Early variations of chess date back to 3000 B.C. and were considered to be one of the first forms of war games.<sup>336</sup> 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.<sup>337</sup> 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.<sup>338</sup> 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.<sup>339</sup> 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.<sup>340</sup>

---

THE WORLD: A HISTORY OF SIMULATING WARS, PEOPLE AND FANTASTIC ADVENTURES, FROM CHESS TO ROLE-PLAYING GAMES (2012).

334. 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.”).

335. 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.”).

336. See MCHUGH, *supra* note 333, at 27.

337. DEP’T 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”).

338. Thomas B. Allen, *Twilight Zone in the Pentagon*, in THE COLD WAR: A MILITARY HISTORY 230, 230–34 (Robert Cowley ed., 2005).

339. 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).

340. See ANTHONY H. CORDESMAN & ASHLEY HESS, THE EVOLVING MILITARY BALANCE IN THE KOREAN PENINSULA AND NORTHEAST ASIA, VOLUME II:

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.<sup>341</sup>

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.<sup>342</sup> 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.<sup>343</sup> 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.<sup>344</sup> 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.<sup>345</sup> 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.<sup>346</sup>

---

CONVENTIONAL BALANCE, ASYMMETRIC FORCES, AND US FORCES 178 (2013).

341. *Id.*

342. See DEPT 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).

343. See NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 151–53 (2004); LAWRENCE WRIGHT, THE LOOMING TOWERS: AL-QAEDA AND THE ROAD TO 9/11 348 (2005).

344. See *generally* MICAH ZENKO, RED TEAM: HOW TO SUCCEED BY THINKING LIKE THE ENEMY (2015).

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).

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.<sup>347</sup> 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.<sup>348</sup> 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.<sup>349</sup>

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.<sup>350</sup> 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.”<sup>351</sup> To date, it is difficult to say

---

35 (discussing the need to gather better information in connection with combatting terrorist financing); SUSAN W. BRENNER, *CYBERTHREATS: THE EMERGING FAULT LINES OF THE NATION STATE* 199 (2009) (suggesting that civilian firms should take a more active role in cyberwarfare in partnership with the military).

347. WEINER, *supra* note 17, at 13–14.

348. See Nicole Hong, *Pittsburgh at Fore of Cybercrime Fight*, WALL ST. J., Aug. 14, 2015, at A3; NAT’L CYBER-FORENSICS & TRAINING ALL., <https://www.ncfta.net> (last visited Mar. 7, 2016).

349. See *Fact Sheet: Quantum Dawn 3*, SIFMA 1, <http://www.sifma.org/uploadedfiles/services/bcp/quantum-dawn-fact-sheet.pdf> (last visited Mar. 7, 2016); *Quantum Dawn 3 After-Action Report*, SIFMA 3 (Nov. 23, 2015), <http://www.sifma.org/uploadedfiles/services/bcp/quantumdawn-3-after-action-report.pdf>.

350. See, e.g., Lawrence A. Cunningham & David Zaring, *The Three or Four Approaches to Financial Regulation: A Cautionary Analysis Against Exuberance in Crisis Response*, 78 GEO. WASH. L. REV. 39, 49–59 (2009) (describing the ad-hoc responses of policymakers following the recent financial crisis).

351. RICHARD M. NIXON, *SIX CRISES* 235 (1962) (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.<sup>352</sup> 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.<sup>353</sup>

### 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.

---

er).

352. See, e.g., U.S. GOV'T 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).