BUSINESS WARFARE

TOM C.W. LIN

BUSINESS WARFARE

TOM C.W. LIN*

Abstract: Businesses are under attack. State and non-state adversaries are assaulting companies using drones, mercenaries, cyberweapons, sanctions, and restrictions. Instead of military installations and government institutions, private firms are often the preferred targets in this mode of warfare. Instead of soldiers and squadrons with bullets and bombs, the weapons of choice are frequently economic hostilities and cyberattacks. This is the new war on business.

This Article offers an original examination of contemporary business warfare, its growing importance to national and corporate affairs, and the need for better pragmatic approaches to understanding and addressing its rising threat to our economic stability, national security, and social welfare. It begins by providing an overview of the business theater of war, investigating the combatants, targets, and weapons. Next, this Article analyzes recent episodes of business warfare involving the United States, Russia, Iran, Saudi Arabia, and China to ground the theoretical discussion in the real world. These case studies illustrate the complex matrix of considerations posed by business warfare. The Article then contends with the fundamental legal and practical tensions of economic impact, business hostilities, cyberattacks, and non-state actors that emanate from business warfare. Finally, moving from problems to solutions, this Article proposes three workable initiatives to better protect firms and nations against the risks of business warfare. Specifically, it argues for robust business war games, smart cybersecurity guidance and incentives, as well as greater supply chain and market diversification. Ultimately, this Article aspires to provide a practical blueprint for government and corporate leaders to reflect, plan, and act with more urgency about the consequential realities of business warfare.

INTRODUCTION

Nations and businesses compete.[1] They clash with one another.[2] They contend for critical supplies, scarce talent, market share, know-how, influence,

* Jack E. Feinberg Chair Professor of Law, Temple University Beasley School of Law. Distinguished Academic Fellow, Center for Law, Economics & Finance, The George Washington University. Many thanks to Anjali Deshpande, Benton Heath, Duncan Hollis, William Magnuson, Harvey Rishikof, Guillermo Garcia Sanchez, as well as conference/workshop participants at the National Business Law Scholars Conference, New York University School of Law, and Texas A&M University School of Law for helpful comments and exchanges. Additionally, I am grateful to Kelly Duffner, Kevin Rajan, and Matthew Sherman for their extraordinary research assistance.

and power in an interconnected world.[3] This competition has been made self-evident during the COVID-19 pandemic, as governments and corporations race to find therapies, vaccines, and policies to curb the deadly spread of a mutating virus.[4] Some of this competition is friendly, cooperative, and mutually beneficial.[5] Other competition is hostile, contentious, and imperious.[6] In recent years, this competition between and among nations and businesses has grown alarmingly and increasingly adversarial and combative as nation-states and non-state actors target specific businesses for attacks, sanctions, and recriminations with new intensity and methods.[7] This growing contemporary war on business has serious legal, economic, and social implications.

Over the last decade or so, the world has witnessed the emergence of this new mode of business warfare.[8] For example, the United States banned Huawei, one of China's largest and most prominent technology companies, from doing business in the United States due to national security concerns.[9] Foreign drones affiliated with Iran attacked oil installations of state-owned

---

[1] *See generally* JOSEPH E. STIGLITZ, GLOBALIZATION AND ITS DISCONTENTS REVISITED: ANTI-GLOBALIZATION IN THE ERA OF TRUMP 28 (2018) (describing "a system of globalization under which countries competed in every way possible to attract business"); MICHAEL E. PORTER, ON COMPETITION, at xi (2008) ("Competition is pervasive, whether it involves companies contesting markets, countries coping with globalization, or social organizations responding to societal needs.").

[2] *See* DAVID ROTHKOPF, POWER, INC.: THE EPIC RIVALRY BETWEEN BIG BUSINESS AND GOVERNMENT—AND THE RECKONING THAT LIES AHEAD 195 (2012) ("[C]orporations have grown in influence worldwide and in every instance have played a role in paring away key prerogatives of the state.").

[3] *See* THOMAS J. WRIGHT, ALL MEASURES SHORT OF WAR: THE CONTEST FOR THE TWENTY-FIRST CENTURY AND THE FUTURE OF AMERICAN POWER 130 (2017) ("Countries are competing with each other but they are also closely linked; consequently, they are gradually exploring how to use these linkages to their own advantage.").

[4] *See* David E. Sanger, David D. Kirkpatrick, Sui-Lee Wee & Katrin Bennhold, *A Global Race to Figure Out a Silver Bullet*, N.Y. TIMES, Mar. 20, 2020, at A1; Yasmeen Serhan, *Vaccine Nationalism Is Doomed to Fail*, THE ATLANTIC (Dec. 8, 2020), https://www.theatlantic.com/international/archive/2020/12/vaccine-nationalism-doomed-fail/617323/ [https://perma.cc/7LX3-TNRA].

[5] *See* DANIEL W. DREZNER, THE SYSTEM WORKED: HOW THE WORLD STOPPED ANOTHER GREAT DEPRESSION 24–27 (2014) (discussing how nations worked together to solve a global financial crisis in the years following 2008).

[6] *See* DANIEL YERGIN, THE NEW MAP: ENERGY, CLIMATE, AND THE CLASH OF NATIONS 423 (2020) ("The world has become more fractured, with a resurgence of nationalism and populism and distrust, great power competition, and with a rising politics of suspicion and resentment.").

[7] *See* J. Benton Heath, *The New National Security Challenge to the Economic Order*, 129 YALE L.J. 1020, 1024 (2020) ("Major geopolitical disputes now play out within trade and investment institutions rather than outside them.").

[8] *See* JUAN C. ZARATE, TREASURY'S WAR: THE UNLEASHING OF A NEW ERA OF FINANCIAL WARFARE 384 (2013) ("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.").

[9] Steve Lohr, *U.S. Moves to Ban Huawei from Government Contracts*, N.Y. TIMES, Aug. 8, 2019, at B6.

Saudi Aramco, one of the most valuable companies in the world.[10] Members of China's military hacked into the American data corporate giant, Equifax, to gather private, sensitive information about American officials and intelligence officers for bribery and blackmail.[11] North Korea initiated an unprecedented attack on Sony in response to a movie portraying North Korea's president in an unflattering manner.[12] Hackers affiliated with Russia targeted large American corporations and large swaths of the federal government.[13] Regardless of form, motivation, and severity, these hostilities against individual businesses raise critical, interlocking questions about law, commerce, society, and warfare.

This Article reviews the contemporary war on business, its growing importance to corporate and national affairs, and the pressing need for better, pragmatic approaches to understanding and addressing these rising threats to our economic stability, national security, and social welfare. This Article offers a descriptive and normative examination of the contemporary acts of warfare and aggression that many businesses currently face. It explores the combatants, targets, and weapons of this conflict in the present-day context; highlights critical legal and practical tensions; and proposes workable initiatives to better protect business stakeholders and nations against the looming threats presented by this new war on business.

Building and drawing on the author's prior works,[14] and a rich, interdisciplinary literature relating to law, management, history, international relations, national security, and cybersecurity, this Article seeks to make three contributions.[15] First, this Article aims to provide an original preliminary narrative for

---

[10] Ben Hubbard, Palko Karasz & Stanley Reed, *Saudi Oil Supply Is Put in Danger by Drone Strikes*, N.Y. TIMES, Sept. 15, 2019, at A1.

[11] Katie Benner, *Justice Dept. Charges 4 Chinese in Equifax Hack*, N.Y. TIMES, Feb. 11, 2020, at A1.

[12] *See* BEN BUCHANAN, THE HACKER AND THE STATE: CYBER ATTACKS AND THE NEW NORMAL OF GEOPOLITICS 70–80 (2020) (chronicling the cyberattack on Sony by North Korea).

[13] Nicole Perlroth, David E. Sanger & Julian E. Barnes, *Russian-Owned Software Company Eyed as Entry Point for Wide Breach*, N.Y. TIMES, Jan. 7, 2021, at A20.

[14] Some of the ideas discussed in this Article stem from and build on research and base material included in the author's previous work, edited and published by the *Minnesota Law Review* in 2016. *See* Tom C.W. Lin, *Financial Weapons of War*, 100 MINN. L. REV. 1377 (2016) (discussing the growing importance and capabilities of financial weapons).

[15] *See id.* at 1377–78 (discussing cybersecurity); *see, e.g.*, IVAN ARREGUÍN-TOFT, HOW THE WEAK WIN WARS: A THEORY OF ASYMMETRIC CONFLICT 2–15 (2005) (history and international relations); CHRISTIAN BROSE, THE KILL CHAIN: DEFENDING AMERICA IN THE FUTURE OF HIGH-TECH WARFARE 25–27 (2020) (cybersecurity); JENNIFER RIEL & ROGER L. MARTIN, CREATING GREAT CHOICES: A LEADER'S GUIDE TO INTEGRATIVE THINKING 122 (2017) (management); DAVID E. SANGER, THE PERFECT WEAPON: WAR, SABOTAGE, AND FEAR IN THE CYBER AGE 121–25 (2018) (cybersecurity and international relations); Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1062–63 (2014) (cybersecurity); Mehrsa Baradaran, *Regulation by Hypothetical*, 67 VAND. L. REV. 1247, 1319 (2014) (law); Kristen E. Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520, 522–26 (2020) (law and cybersecurity); Oona A. Hathaway et al.,

explaining and understanding contemporary business warfare in an integrative manner that cuts across disciplines. Second, building upon this narrative, this Article aims to identify and analyze larger legal and practical tensions relating to business warfare given the crosscutting concerns of global economics, national security, and corporate governance. Third, it aims to offer a set of pragmatic proposals for national policy-makers and corporate stakeholders seeking to address the important consequences posed by business warfare.[16]

In pursuit of these objectives, this Article is mindful of the serious and varied national security and military considerations implicated by contemporary business warfare, but it aims to provide a more crosscutting, civilian-oriented perspective.[17] At the same time, the Article is also cognizant of the longstanding, traditional legal perspective that generally views economic and financial hostilities targeting businesses as actions that fall short of traditional categorizations and terminologies of war.[18] Nevertheless, this Article argues for a more nuanced, novel view on the matter as the traditional boundaries of private business, public policy, and national security blur and break down in a

---

The Law of Cyber-Attack, 100 CALIF. L. REV. 817, 837 (2012) (law and cybersecurity); Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1534–36 (2010) (history and cybersecurity); Neal K. Katyal & Laurence H. Tribe, Essay, *Waging War, Deciding Guilt: Trying the Military Tribunals*, 111 YALE L.J. 1259, 1260 (2002) (history and national security); Harold Hongju Koh, Remarks, *The State Department Legal Adviser's Office: Eight Decades in Peace and War*, 100 GEO. L.J. 1747, 1772 (2012) (international relations); Tom C.W. Lin, *The New Market Manipulation*, 66 EMORY L.J. 1253, 1287–93 (2017) (law and cybersecurity); Heath P. Tarbert, *Modernizing CFIUS*, 88 GEO. WASH. L. REV. 1477, 1495 (2020) (national security); Andrew Verstein, *The Corporate Governance of National Security*, 95 WASH. U. L. REV. 775, 777–80 (2018) (national security).

[16] *See infra* Part IV.

[17] For a small sampling of the rich national security and military-oriented writings related to business warfare, see, for example, CHRIS NISSEN, JOHN GRONAGER, ROBERT METZGER & HARVEY RISHIKOF, DELIVER UNCOMPROMISED: A STRATEGY FOR SUPPLY CHAIN SECURITY AND RESILIENCE IN RESPONSE TO THE CHANGING CHARACTER OF WAR 7–14 (2018), https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-26AUG2019.pdf [https://perma.cc/L724-AMA9]; Robert Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 5 J. NAT'L SEC. L. & POL'Y 539, 542–45 (2012); Gerhard Wheeler, *Operational Resilience: Applying the Lessons of War*, CAPCO INST. J. FIN. TRANSFORMATION, May 2021, at 134, 134–35; Gary Corn, *Cyber Operations and the Imperfect Art of "Translating" the Law of War to New Technologies*, LIEBER INST. W. POINT: ARTICLES OF WAR (Sept. 3, 2020), https://lieber.westpoint.edu/cyber-operations-imperfect-translating-law-war-new/ [https://perma.cc/NE7U-DJMH].

[18] *See, e.g.*, NILS MELZER, 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), https://www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf [https://perma.cc/3N56-5FV5]; 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, 422 (2011) ("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.").

new age of global commerce and conflict.[19] The ineffable nature of modern global conflicts renders traditional dictions and doctrines of warfare insufficient along multiple vectors, and readily makes stale attempts at drawing new theoretical bright lines.[20] While law and policy might be lacking in appropriately cogent categories and clear terminology for what is happening, the realities of the world are not lacking in troubling cases and the need for practical—albeit inelegant—proposals. In response to that void, this Article aspires to provide an original, pragmatic mirror and searchlight for reflecting, conceptualizing, and guarding against the consequential realities of contemporary business warfare.

This Article constructs this mirror and searchlight in four parts. Part I reveals the emerging form of business warfare.[21] It describes contemporary business warfare as a form of asymmetrical warfare that can be waged by nation-states and non-state actors against their adversaries by targeting individual businesses and industries. It identifies the business targets, combatants, and weapons used in business warfare. It also explains why the United States and its businesses are particularly vulnerable to this form of warfare. Overall, this Part provides a broad conceptual survey of the business theater of war.

Moving from conceptual to concrete, Part II examines recent episodes of business warfare.[22] It studies actions by the United States, Russia, Iran, and China to reflect and highlight the novel complexities involved in this new form of hostility. In analyzing these recent episodes, this Article foretells the practical and legal challenges posed by business warfare.

Part III grapples with those practical and legal challenges.[23] It argues that business warfare raises serious implications for an interconnected global economy. It then contends that business warfare tests longstanding legal rules and norms concerning economic hostilities, cyberattacks, and non-state actors. It deconstructs and highlights the structural deficiencies of traditional conventions on war and armed conflict as they relate to business warfare.[24]

Advancing from reflection and examination to protection and preemption, Part IV offers an early searchlight for navigating and addressing the rising

---

[19] *See* Heath, *supra* note 7, at 1032 (observing "the growing overlap between national security policy and the ordinary trade and investment rules since the end of the Cold War").

[20] *See, e.g.*, JOHN SEXTON WITH THOMAS OLIPHANT & PETER J. SCHWARTZ, BASEBALL AS A ROAD TO GOD: SEEING BEYOND THE GAME 211 (2013) (defining ineffable as "[t]hat which we know through experience rather than through study, that which ultimately is indescribable in words yet is palpable and real").

[21] *See infra* notes 27–171 and accompanying text.

[22] *See infra* notes 172–238 and accompanying text.

[23] *See infra* notes 239–320 and accompanying text (finding that the laws and norms of traditional military conflict did not account for cyber or business warfare when they were originally drafted).

[24] *See infra* notes 265–320 and accompanying text.

threats of business warfare.[25] It recommends three workable, near-term action items for public policy-makers and business stakeholders to adopt while key nations in the global community deliberate larger, international policy and legal matters. In particular, it advocates for robust business war games, smart cybersecurity guidance and incentives, and supply chain and market diversification to sidestep the abyss of open international and geopolitical issues and focus on the urgent present.

This Article ends with a short conclusion that reflects on the looming dangers of business warfare, and looks forward optimistically to the hope of mitigating business warfare threats to create a safer and more prosperous global community.[26]

I. THE BUSINESS THEATER OF WAR

The global marketplace is the emerging new theater of contemporary global conflict. Issues and concerns about national security, economic prosperity, and corporate governance have become more intertwined.[27] Whereas traditional wars have been contested in air, land, and sea, the skirmishes of today are frequently fought in a new business theater of war.[28] First, Section A of this Part delves into the business theatre of war and the difficulties associated with business warfare's asymmetrical nature.[29] Next, Section B explores the familiar combatants involved in business warfare and their preferred targets.[30] Lastly, Section C analyzes the types of cyberweapons, old and new, that today's combatants utilize in their attacks.[31]

A. The New Asymmetrical Warfare

Contemporary business warfare represents a new variation of asymmetrical warfare that is especially prevalent against the United States and American businesses.[32] This asymmetry manifests along multiple vectors in business

---

[25] *See infra* notes 321–384 and accompanying text.

[26] *See infra* notes 347–384 and accompanying text (suggesting practical solutions and ideas that can help protect businesses from business warfare).

[27] *See* Verstein, *supra* note 15, at 777–80 (discussing the growing links between the national security agencies of governments and private corporations).

[28] ZARATE, *supra* note 8, at 384.

[29] *See infra* notes 32–58 and accompanying text.

[30] *See infra* notes 59–100 and accompanying text.

[31] *See infra* notes 101–171 and accompanying text.

[32] *See, e.g.*, SCOTT JASPER, RUSSIAN CYBER OPERATIONS: CODING THE BOUNDARIES OF CONFLICT 28–32 (2020) (discussing Russian asymmetric warfare tactics against the United States); NISSEN ET AL., *supra* note 17, at 28–29 (discussing the public-private blended asymmetrical nature of modern warfare).

warfare.[33] First, there is an asymmetry between the force of a nation-state or non-state actor and that of a business entity, or between warring nation-states.[34] For instance, if North Korea decided to unleash an attack on Apple operations around the world, there would exist a significant imbalance between Apple's capabilities and defenses relative to those possessed by North Korea. No private business, no matter how wealthy or sophisticated, can really fight on equal footing against a nation-state with military armed forces. Second, asymmetry exists in the economic power and prowess of adversaries.[35] For example, a poorer country could attack many business targets of an economically stronger country.

Third, asymmetry exists in the techno-network effects of business warfare, namely between technologically advanced, well-networked countries versus less technologically advanced and networked countries.[36] This means that an attack on the businesses of some countries will have greater ripple effects, both in that country and beyond. For example, on one hand, an attack that significantly disrupts or disables a highly networked American company like Goldman Sachs or Microsoft would have deleterious economic effects within the United States and around the world.[37] On the other hand, an attack on the largest state-owned banks or technology companies in North Korea would likely not be as impactful because North Korea is not as networked domestically, and is not as interlinked with the global community.[38]

---

[33] *See, e.g.*, ARREGUÍN-TOFT, *supra* note 15, at 2–15 (providing an overview of asymmetric conflicts among nation-states).

[34] *Id.* at 2–15.

[35] David L. Buffaloe, *Defining Asymmetric Warfare*, *in* THE LAND WARFARE PAPERS 2006, at 3, 22 (Inst. of Land Warfare, Assoc. of the U.S. Army, Land Warfare Paper No. 58, 2006), https://www.ausa.org/sites/default/files/LWP-58-Defining-Asymmetric-Warfare.pdf [https://perma.cc/B7X3-T8MJ].

[36] Ian Bremmer, *The Technopolar Moment: How Digital Powers Will Reshape the Global Order*, FOREIGN AFFS. (Nov./Dec. 2021), https://www.foreignaffairs.com/articles/world/2021-10-19/ian-bremmer-big-tech-global-order [https://perma.cc/4AGR-AAEV].

[37] *See, e.g.*, TED KOPPEL, LIGHTS OUT: A CYBERATTACK, A NATION UNPREPARED, SURVIVING THE AFTERMATH 55–75 (2015) (discussing how cyberattacks on critical networks managed by various types of companies within the United States could have deleterious effects domestically and internationally); Jason Healey, Patricia Mosser, Katheryn Rosen & Alexander Wortman, *The Ties That Bind: A Framework for Assessing the Linkage Between Cyber Risks and Financial Stability*, CAPCO INST. J. FIN. TRANSFORMATION, May 2021, at 94, 94–95 (explaining how cyber risks can create systemic financial instability); Elizabeth A. Rowe, *RATs, TRAPs, and Trade Secrets*, 57 B.C. L. REV. 381, 384 (2016) (documenting the rise of cyber espionage against American companies and the estimated $1 trillion in intellectual property losses in 2009 alone).

[38] *See* EMMA CHANLETT-AVERY, LIANA W. ROSEN, JOHN W. ROLLINS & CATHERINE A. THEOHARY, CONG. RSCH. SERV., R44912, NORTH KOREAN CYBER CAPABILITIES: IN BRIEF 1 (2017) (describing North Korea as having "one of the smallest Internet presences in the world"); Scott Snyder, *North Korea's Challenge of Regime Survival: Internal Problems and Implications for the Future*, 73 PAC. AFFS. 517, 517 (2000) (documenting North Korea's inadequate and destitute infrastructure).

The United States is particularly vulnerable to the asymmetrical nature of business warfare, given the prominence of American business on the global stage. By engaging in business warfare, enemies that could not otherwise win traditional wars of soldiers and arms with the United States, given its superpower strengths, now seek to attack American business interests directly to inflict harm on American national security and economic welfare.[39] Many prominent American businesses, with their size, value, and influence, serve as attractive targets for enemies of the state who would otherwise be reticent to engage the United States in traditional battles.[40]

Despite its struggles with the unfolding pandemic, the United States remains the world's lone superpower.[41] Its economic power, military might, and global influence remains second to none. In terms of economic power, at the end of 2020, the gross domestic product (GDP) of the United States stood at around $21 trillion, despite the global recession caused by the pandemic.[42] To put this in perspective, China's GDP, which was the second largest, stood just under $15 trillion; Japan's GDP, which was the third largest, was around $5 trillion; and Germany, which was the fourth largest GDP, was around $4 trillion.[43] Moreover, the U.S. dollar is the world's reserve currency and the most trusted investment during times of distress, accounting for over 60% of foreign exchange reserves.[44] Almost 90% of trading around the world uses the U.S. dollar.[45] Additionally, American capital markets dominate global finance.[46]

---

[39] *See, e.g.*, Farhad Manjoo, Opinion, *We Really Must Stop Starting Wars*, N.Y. TIMES (Jan. 9, 2020), https://www.nytimes.com/2020/01/09/opinion/iran-war-us.html [https://perma.cc/Y8VM-ZJ74] ("Technology is turning armed conflict into an endeavor increasingly dominated by what war scholars call 'asymmetric warfare'—meaning that weaker powers like Iran can now marshal so much strength that they are no longer very weak, exacting a mighty cost of victory even to the world's pre-eminent global superpower.").

[40] *See* ROBERT D. BLACKWILL & JENNIFER M. HARRIS, WAR BY OTHER MEANS: GEOECONOMICS AND STATECRAFT 1–3 (2016) (discussing general economic warfare against American interests by foreign states); BUCHANAN, *supra* note 12 (detailing the targeting of American companies by foreign adversaries).

[41] *See* Ed Yong, *How the Pandemic Defeated America*, THE ATLANTIC, https://www.theatlantic.com/magazine/archive/2020/09/coronavirus-american-failure/614191/ [https://perma.cc/TN79-J4U9] (Aug. 4, 2020) (documenting the United States' struggles during the coronavirus pandemic); Robert Kagan, *A Superpower, Like It or Not: Why Americans Must Accept Their Global Role*, FOREIGN AFFS. (Mar./Apr. 2021), https://www.foreignaffairs.com/articles/united-states/2021-02-16/superpower-it-or-not [https://perma.cc/9CQT-MNZR] (describing the United States as the lone superpower).

[42] News Release, Bureau of Econ. Analysis, Gross Domestic Product, (Third Estimate), GDP by Industry, and Corporate Profits, Fourth Quarter and Year 2020 (Mar. 25, 2021), https://www.bea.gov/news/2021/gross-domestic-product-third-estimate-gdp-industry-and-corporate-profits-4th-quarter-and [https://perma.cc/PNP2-NLLV].

[43] WORLD BANK, GROSS DOMESTIC PRODUCT 2020 (2021), https://databank.worldbank.org/data/download/GDP.pdf [https://perma.cc/3KYW-XVUX].

[44] *See* ZARATE, *supra* note 8, at 9 (describing the history of financial warfare, and how the U.S. dollar has come to serve as the dominant currency and trusted global currency reserve); Kimberly

In terms of military might, the United States possesses the world's best trained military, most sophisticated weapons, and largest defense budgets.[47] The United States spends about $700 billion annually on defense.[48] To put that in context, U.S. defense spending amounts to 38% of global defense spending, and it represents more defense expenditures than the next ten countries combined.[49]

Considering global influence, the United States remains the most influential country on the global stage.[50] American economic, military, and diplomatic powers continue to steer global agendas and policies. Moreover, American soft power in terms of ideas, entertainment, and culture continues to play a leading role around the world.[51]

Given its structural advantages in terms of economy, military, and influence, adversaries of the United States resort to battles in unconventional theaters of warfare, using alternative tactics, to avoid an almost certain defeat in the traditional terrain of war. In recent years, adversaries have resorted to waging asymmetrical warfare against specific American businesses and business interests, using these as proxies for the country, to gain an advantage in conflicts and disputes.[52]

Amadeo, *Why the US Dollar Is the Global Currency*, THE BALANCE, https://www.thebalance.com/world-currency-3305931 [https://perma.cc/6UBH-H8FP] (July 23, 2020) ("As of the fourth quarter of 2019, [the U.S. dollar made] up over 60% of all known central bank foreign exchange reserves.").

[45] MONETARY & ECON. DEP'T, BANK FOR INT'L SETTLEMENTS, TRIENNIAL CENTRAL BANK SURVEY: FOREIGN EXCHANGE TURNOVER IN APRIL 2019, at 3 (2019), https://www.bis.org/statistics/rpfx19_fx.pdf [https://perma.cc/E6T4-9XZB]

[46] *See* PWC & THE ECONOMIST INTEL. UNIT, CAPITAL MARKETS IN 2030: THE FUTURE OF EQUITY CAPITAL MARKETS 5, 10 (2019) https://www.pwc.com/gx/en/audit-services/capital-market/publications/capital-markets-2030.pdf [https://perma.cc/68M4-GENA] (reviewing stock exchanges and the strong growth of U.S. exchanges compared to their Asian and European counterparts).

[47] *See, e.g.*, Poppy Koronka, *The 20 Most Powerful Military Forces in the World*, NEWSWEEK (Aug. 24, 2021), https://www.newsweek.com/most-powerful-military-forces-world-america-china-russia-1621130 [https://perma.cc/VG83-SDZM] (ranking the United States military as the most powerful); *2021 Military Strength Ranking*, GLOB. FIREPOWER, https://www.globalfirepower.com/countries-listing.php [https://perma.cc/HQ6T-57RF] (same).

[48] NAN TIAN ET AL., STOCKHOLM INT'L PEACE RSCH. INST., FACT SHEET: TRENDS IN WORLD MILITARY EXPENDITURE, 2019, at 2 (2020), https://www.sipri.org/sites/default/files/2020-04/fs_2020_04_milex_0_0.pdf [https://perma.cc/XA6Y-4R2X].

[49] *Id.* at 2, 3; *U.S. Defense Spending Compared to Other Countries*, PETER G. PETERSON FOUND. (July 9, 2021), https://www.pgpf.org/chart-archive/0053_defense-comparison [https://perma.cc/4YQU-93NH].

[50] *See, e.g.*, *The USA's International Influence: The Role of the US as a World Power*, BBC: BITESIZE, https://www.bbc.co.uk/bitesize/guides/z6frqp3/revision/2 [https://perma.cc/XHD4-XG78] (reviewing the United States' global influence); *The USA's International Influence: Involvement in International Organisations*, BBC: BITESIZE, https://www.bbc.co.uk/bitesize/guides/z6frqp3/revision/3 [https://perma.cc/XF4M-E928] (same).

[51] *See* JOSEPH S. NYE, JR., SOFT POWER: THE MEANS TO SUCCESS IN WORLD POLITICS 33–41 (2004) (chronicling the United States' soft power and cultural influence on the rest of the world).

[52] *See, e.g.*, *infra* notes 201–205 and accompanying text (describing the cyberattacks attributed to Iran against the U.S. financial industry).

This form of business warfare echoes asymmetrical wars of the past.[53] During the Vietnam War, the Viet Cong of North Vietnam waged asymmetrical warfare against the United States and South Vietnam for years, using guerrilla tactics to exhaust and defeat a much more powerful military.[54] The Vietnam War also represented a form of proxy warfare whereby North Vietnam and South Vietnam served as stand-ins for the United States' fight against the spread of communism led by the Soviet Union.[55] More recently, on September 11, 2001, Al-Qaeda terrorists attacked the United States using commercial airplanes in an audacious act of asymmetrical warfare against an exponentially larger, stronger opponent.[56]

In sum, although traditional asymmetrical warfare still exists, the business arena has emerged as a new theater of war for such fights among geopolitical actors. Whereas traditional warfare tactics have often become too bloody, costly, and futile, attacks via business warfare have grown more attractive and prevalent.[57] To be clear, although the United States and its businesses are frequently the targets of such attacks, other geopolitical players engage in and initiate business warfare as well, including the United States itself.[58]

B. The Targets

Businesses are often prime and preferred targets in modern conflicts. They are relatively exposed and unguarded compared to traditional military

---

[53] *See generally* John F. Kennedy, President, United States Military Academy Commencement Address (June 6, 1962), https://www.americanrhetoric.com/speeches/jfkwestpointcommencement speech.htm [https://perma.cc/29PS-NNVZ] ("[Asymmetrical warfare] is another type of war, new in its intensity, ancient in its origin—war by guerrillas, subversives, insurgents, assassins, war by ambush instead of by combat; by infiltration, instead of aggression, seeking victory by eroding and exhausting the enemy instead of engaging him.").

[54] *See* ARREGUÍN-TOFT, *supra* note 15, at 155–60 (analyzing the asymmetric warfare tactics used during the Vietnam War); H.R. MCMASTER, DERELICTION OF DUTY: LYNDON JOHNSON, ROBERT MCNAMARA, THE JOINT CHIEFS OF STAFF, AND THE LIES THAT LED TO VIETNAM 157–60 (1997) (describing the guerrilla warfare by the North Vietnamese against a large, superior American military).

[55] MICHAEL LIND, VIETNAM: THE NECESSARY WAR 4–5 (1999).

[56] *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 1–14 (2004), https://www.9-11commission.gov/report/911Report.pdf [https://perma.cc/RYV8-8HVA] (reporting how terrorists committed the September 11th attacks through the hijacking of commercial airplanes); MICHAEL W.S. RYAN, DECODING AL-QAEDA'S STRATEGY: THE DEEP BATTLE AGAINST AMERICA 106–07 (2013) (describing the nature of the asymmetrical warfare between Al-Qaeda and the United States).

[57] *See* T. Casey Fleming, Eric L. Qualkenbush & Anthony M. Chapa, Professional Commentary, *The Secret War Against the United States*, CYBER DEF. REV., Fall 2017, at 25, 26–28 (reviewing China's asymmetrical approach through non-traditional military means such as business warfare).

[58] *See, e.g.*, David E. Sanger & Nicole Perlroth, *U.S. Escalates Online Attacks on Russia's Power Grid*, N.Y. TIMES (June 15, 2019), https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html [https://perma.cc/VW5S-7L8R] (describing U.S. cyberattacks on Russia).

targets. Businesses normally do not possess military-grade defensive or offensive capabilities comparable to those of nation-states. And perhaps most importantly, a successful attack on a key business can have a devastating impact on an adversary.[59]

This Section discusses four crosscutting categories of businesses that are particularly noteworthy targets: (1) high-value companies;[60] (2) state-owned enterprises;[61] (3) nationally significant businesses;[62] and (4) politically connected businesses.[63] To be clear, a business can fall into multiple categories. For instance, Saudi Aramco, the state-owned energy company of Saudi Arabia, is one of the largest and most valuable companies in the world.[64] By virtue of being the largest energy company in the world and being owned by the Saudi ruling family, Saudi Aramco is also a nationally significant as well as a politically connected business.[65]

1. High-Value Companies

Considering high-value companies first, these make for obvious targets because a successful attack against one could have a devastating psychological and economic impact on an adversary. Today's largest high-value companies are akin to nation-states in many ways.[66] The revenues and market cap of the largest technology companies in the world rival and surpass the GDP of many large nations.[67] For example, Apple, the most valuable company in the world, had a 2020 fiscal year revenue of nearly $275 billion, and it had a market cap

[59] *See, e.g.*, KOPPEL, *supra* note 37, at 55–75 (outlining the serious consequences that an attack can have on the U.S. financial system); Healey et al., *supra* note 37, at 94–95 (explaining how a cyberattack can create grave consequences on the United States' financial system).

[60] *See infra* notes 66–81 and accompanying text.

[61] *See infra* notes 82–88 and accompanying text.

[62] *See infra* notes 89–96 and accompanying text.

[63] *See infra* notes 97–100 and accompanying text.

[64] *See* Jasper Jolly & Jillian Ambrose, *Saudi Aramco Becomes Most Valuable Listed Company in History*, THE GUARDIAN (Dec. 11, 2019), https://www.theguardian.com/business/2019/dec/11/saudi-aramco-shares-soar-as-it-becomes-world-largest-listed-company [https://perma.cc/77AF-QTPT] (describing Saudi Aramco and its initial public offering (IPO)).

[65] *See* Gretchen Frazee, *What Americans Should Know About Saudi Aramco's IPO*, PBS NEWSHOUR (Dec. 11, 2019), https://www.pbs.org/newshour/economy/making-sense/what-americans-should-know-about-saudi-aramcos-ipo [https://perma.cc/N53K-ZP4W] (reporting that after its IPO, the Saudi government still holds 98.5% of the company's shares).

[66] *See* ROTHKOPF, *supra* note 2, at 195 ("[C]orporations have been able to gain unprecedented power relative to the states that once gave life to them.").

[67] *See* Raul Amoros, *Who Is More Powerful—Countries or Companies?*, HOWMUCH.NET (July 11, 2019), https://howmuch.net/articles/putting-companies-power-into-perspective [https://perma.cc/3QMQ-CWVE] (comparing companies' market caps against countries' GDPs).

exceeding $2 trillion.[68] This means that Apple's 2020 market cap would have placed it as the tenth largest nation in the world in terms of GDP, ahead of countries like Italy, Russia, South Korea, Australia, and Spain.[69] By early 2022, Apple's market cap had grown to exceed $3 trillion.[70]

Additionally, the global reach and user base of some companies outnumber the population of many nation-states. Meta/Facebook (Facebook), for instance, has almost 2.9 billion monthly active users on its namesake platform.[71] This figure rises to over 3.5 billon active users if one includes its other platforms like WhatsApp, Instagram, and Messenger.[72] If Facebook were a country and active monthly users its headcount, it would be the largest country in the world.[73] Facebook also has created its own currency system and an independent oversight board that acts like its own version of the Supreme Court to adjudicate disputes with its members.[74] These nation-like traits of Facebook have led some to refer to it as "Facebookistan."[75]

Further complicating matters is the fact that many high-value technology companies are becoming more involved in defense and national security work, blurring the traditional lines of public and private.[76] Firms like Microsoft, Am-

---

[68] *See* Jessica Bursztynsky, *Apple Becomes First U.S. Company to Reach a $2 Trillion Market Cap*, CNBC, https://www.cnbc.com/2020/08/19/apple-reaches-2-trillion-market-cap.html [https://perma.cc/SZ74-U9NK] (Aug. 19, 2020, 4:03 PM); *Apple Revenue 2006–2021 | AAPL*, MACROTRENDS, https://www.macrotrends.net/stocks/charts/AAPL/apple/revenue [https://perma.cc/UGJ2-2BYY].

[69] *See* Ami Shah, *Apple at $2 Trillion Market Cap Tops GDP of Italy, Brazil, Canada, Russia and More!*, ECON. TIMES, https://economictimes.indiatimes.com/markets/stocks/news/apple-at-2-trillion-market-cap-tops-gdp-of-italy-brazil-canada-russia-and-more/articleshow/77640249.cms?from=mdr [https://perma.cc/2J7Y-LFC6] (Aug. 20, 2020); WORLD BANK, *supra* note 43 (listing countries' GDPs).

[70] Jack Nicas, *Apple's Valuation Soars to Unheard of $3 Trillion*, N.Y. TIMES, Jan. 4, 2022, at B1.

[71] *See* Mike Isaac, *Facebook Renames Itself Meta*, N.Y. TIMES, https://www.nytimes.com/2021/10/28/technology/facebook-meta-name-change.html [https://perma.cc/ZZB6-VLBV] (Nov. 10, 2021) (discussing the rebranding of Facebook to Meta); Statista Rsch. Dep't, *Facebook: Number of Monthly Active Users Worldwide 2008–2021*, STATISTA (Nov. 1, 2021), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide [https://perma.cc/9ZT7-CGYZ].

[72] Statista Rsch. Dep't, *supra* note 71.

[73] *Compare id.* (stating 2.89 billion active monthly users), *with U.S. and World Population Clock*, U.S. CENSUS BUREAU, https://www.census.gov/popclock/world [https://perma.cc/CA6B-YFGY] (stating that China has the world's largest population, estimated at roughly 1.407 billion people).

[74] *See* Ephrat Livni, *Facebook Says It Wants a 'Fair Shot' in the Crypto Payments Sphere.*, N.Y. TIMES, https://www.nytimes.com/2021/08/18/business/facebook-cryptocurrency-diem-payments.html [https://perma.cc/6CEU-HC5B] (Sept. 17, 2021) (noting Facebook's attempt at creating its own cryptocurrency, "Libra"); FACEBOOK, OVERSIGHT BOARD BYLAWS 5 (2021), https://about.fb.com/wp-content/uploads/2020/01/Bylaws_v6.pdf [https://perma.cc/APU6-RRLS] (providing the bylaws for Facebook's independent oversight board).

[75] Anupam Chander, *Facebookistan*, 90 N.C. L. REV. 1807, 1808, 1813 (2012).

[76] *See* Alex Press, *Big Tech's Unholy Alliance with the Pentagon*, NEW REPUBLIC (Feb. 7, 2019), https://newrepublic.com/article/153044/big-techs-unholy-alliance-pentagon [https://perma.cc/M33D-QDH5] (detailing the big tech companies and their various projects with the U.S. military); Nitasha Tiku, *The Line Between Big Tech and Defense Work*, WIRED (May 21, 2018), https://www.wired.

azon, and Google all provide lucrative and critical services for the U.S. military.[77] This big-tech-military fusion increases the value of these firms. At the same time, it also increases the size of the targets on their backs to adversaries. A successful attack could have the dual benefit of directly hurting American national security and a major American firm, as many adversaries view these high-value companies as extensions of the American government.[78]

If high-value companies are prime targets, then the United States has many rich targets for business warfare. As of early 2021, of the world's ten largest companies by market cap, seven were American companies.[79] When measured by brand value, American companies account for six out of the ten most valuable brands.[80] Although adversaries cannot win a traditional war with the United States, they can engage in business warfare against high-value American companies and cause significant harm to American interests and citizens, given the large and diverse investor population in the United States.[81]

2. State-Owned Enterprises

State-owned enterprises are another category of prime targets in business warfare. According to the Organisation for Economic Co-operation and Development (OECD), state-owned enterprises are "enterprises where the state has

---

com/story/the-line-between-big-tech-and-defense-work/ [https://perma.cc/XC2T-6G9G] (same); Tom C.W. Lin, *Incorporating Social Activism*, 98 B.U. L. REV. 1535, 1558 (2018) (discussing "[t]he convergence of government and business").

[77] *See* April Glaser, *Thousands of Contracts Highlight Quiet Ties Between Big Tech and U.S. Military*, NBC NEWS (July 8, 2020), https://www.nbcnews.com/tech/tech-news/thousands-contracts-highlight-quiet-ties-between-big-tech-u-s-n1233171 [https://perma.cc/M88X-FGKH] (discussing the thousands of contracts that big tech companies have with the U.S. federal government); Jack Poulson, *Reports of a Silicon Valley/Military Divide Have Been Greatly Exaggerated*, TECH INQUIRY (July 7, 2020), https://techinquiry.org/SiliconValley-Military/ [https://perma.cc/W9HJ-A7NU] (discussing the important role tech companies have played in contracting with the federal government); Sharon Weinberger, *Meet America's Newest Military Giant: Amazon*, MIT TECH. REV. (Oct. 8, 2019), https://www.technologyreview.com/2019/10/08/75349/meet-americas-newest-military-giant-amazon/ [https://perma.cc/CHH5-K6YP] (discussing the lucrative contract of the Pentagon's JEDI cloud computing deal).

[78] *See* Kristen E. Eichensehr, *Digital Switzerlands*, 167 U. PA. L. REV. 665, 672 (2019) ("In recent years, major U.S. technology companies have grown into power centers that compete with territorial governments. They are now beginning to be, in some senses, competing sovereigns . . . ." (footnotes omitted)).

[79] *The 100 Largest Companies in the World by Market Capitalization in 2021*, STATISTA (Apr. 16, 2021), https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-value/ [https://perma.cc/B5BJ-G28T].

[80] Katie Jones, *Ranked: The Most Valuable Brands in the World*, VISUAL CAPITALIST (Jan. 30, 2020), https://www.visualcapitalist.com/ranked-the-most-valuable-brands-in-the-world/ [https://perma.cc/EB9C-N6KT].

[81] *See* Tom C.W. Lin, *Reasonable Investor(s)*, 95 B.U. L. REV. 461, 461–62 (2015) (highlighting the depth and diversity of modern investors).

significant control through full, majority, or significant minority ownership."[82] Businesses fitting the definition of state-owned enterprises can serve as extensions of the state. Whereas an adversary might be reluctant to take aggressive action against a military installation or an official governmental office, the commercial nature of state-owned enterprises can create a perceived degree of distance from directly engaging in hostilities with a state.

Today, state-owned enterprises make up some of the largest and most important businesses in the world.[83] According to the International Monetary Fund, in 2020, state-owned enterprises held assets worth forty-five trillion dollars—roughly half of the world's GDP.[84] Many international airline companies like Singapore Airlines and Vietnam Airlines are state-owned enterprises.[85] In China, all of the most critical and valuable businesses are state-owned enterprises, even the publicly-listed ones and including those on American stock exchanges.[86] This includes companies across all sectors of the Chinese economy, from energy to banking to transportation to communications.[87] In many

[82] Jan Sturesson, Scott McIntyre & Nick C. Jones, *Foreword* to PWC, STATE-OWNED ENTERPRISES: CATALYSTS FOR PUBLIC VALUE CREATION? 4 n.1 (2015), https://www.pwc.com/gx/en/psrc/publications/assets/pwc-state-owned-enterprise-psrc.pdf [https://perma.cc/G2H4-SL4G] (paraphrasing the OECD's definition of state-owned enterprises).

[83] *Top 82 Largest State Owned Enterprise Rankings by Total Assets*, SWFI, https://www.swfinstitute.org/fund-rankings/state-owned-enterprise [https://perma.cc/85S3-CNUK].

[84] Vitor Gaspar, Paulo Medas & John Ralyea, *State-Owned Enterprises in the Time of COVID-19*, IMFBLOG (May 7, 2020), https://blogs.imf.org/2020/05/07/state-owned-enterprises-in-the-time-of-covid-19/ [https://perma.cc/6WRA-DY9U].

[85] Jessica Wick, *These Are the Countries That Have National Airlines (and Why America Doesn't)*, SHOWBIZ CHEAT SHEET (May 4, 2018), https://www.cheatsheet.com/culture/these-are-the-countries-that-have-national-airlines-and-why-america-doesnt.html/ [https://perma.cc/RBA3-4JQ5]; Jamie Freed, *Analysis: Cash-Rich Singapore Airlines Positioned for Regional Dominance as Rivals Pullback*, REUTERS, https://www.reuters.com/business/aerospace-defense/cash-rich-singapore-airlines-aims-regional-dominance-rivals-pull-back-2021-07-08/ [https://perma.cc/G2YD-7Z7W] (July 9, 2021) (noting that the majority shareholder of Singapore Airlines is a government-owned investment arm); *Vietnam Airlines Profile*, CAPA CTR. FOR AVIATION, https://centreforaviation.com/data/profiles/airlines/vietnam-airlines-vn [https://perma.cc/7GQB-8PYU] (noting that Vietnam Airlines is majority-owned by the Vietnamese government).

[86] *See* Fan Gang & Nicholas C. Hope, *The Role of State-Owned Enterprises in the Chinese Economy*, *in* US-CHINA 2022: ECONOMIC RELATIONS IN THE NEXT TEN YEARS 4–10 (2013), https://www.chinausfocus.com/2022/wp-content/uploads/Part+02-Chapter+16.pdf [https://perma.cc/W5JR-ZPRN] (reviewing history of China's state-owned enterprises); Amir Guluzade, *The Role of China's State-Owned Companies Explained*, WORLD ECON. F. (May 7, 2019), https://www.weforum.org/agenda/2019/05/why-chinas-state-owned-companies-still-have-a-key-role-to-play/ [https://perma.cc/L6EU-6UY5].[87] *See Top 82 Largest State Owned Enterprise Rankings by Total Assets*, *supra* note 83 (listing, for example, China National Petroleum Corporation (#3), China Mobile Communications Corporation (#6), and China Railway Construction Corporation (#7)).

[87] *See Top 82 Largest State Owned Enterprise Rankings by Total Assets*, *supra* note 83 (listing, for example, China National Petroleum Corporation (#3), China Mobile Communications Corporation (#6), and China Railway Construction Corporation (#7)).

countries around the world, business enterprise is synonymous with state-owned enterprise.

Related to the importance of state-owned enterprises is the rising tide of nationalism in business, as many countries act to promote their own businesses for geopolitical and national security reasons, particularly in the areas of technology, communications, and cybersecurity.[88] This rising nationalism will make state-owned enterprises even larger targets in business warfare as adversaries will increasingly see little to no daylight between the state and their enterprises.

3. Nationally Significant Businesses

Nationally significant businesses are ripe targets for business warfare. These businesses include those engaged in "critical technologies" or "critical infrastructure" like utilities, communications, food supply, financial services, and medicine, among other industries.[89] They also include businesses involved in defense, like Lockheed Martin and Boeing in the United States, as well as businesses that produce so-called "dual-use" products with military and civilian utility.[90] In the United States, nationally significant businesses are designated as part of sixteen "critical infrastructure sectors" by the Cybersecurity and Infrastructure Security Agency.[91] A targeted strike on a nation's critical infrastructure could have a devastating effect on a country's security and economy.

In many countries, including the United States, many nationally significant businesses are privately-owned, in whole or in part, touching on all aspects of daily life.[92] In the United States, electricity, communications, financial services, and defense manufacturing are often provided by large, publicly-

---

[88] *See* Mariana Pargendler, *The Grip of Nationalism on Corporate Law*, 95 IND. L.J. 533, 533, 539, 569 (2020) ("After decades of increased economic integration, nationalistic sentiment and protectionist policies are back in vogue, raising questions about the future of globalization."); Matthew Rosenberg & Ron Nixon, *Kaspersky Lab Software Is Ordered Wiped from Government Computers*, N.Y. TIMES, Sept. 14, 2017, at A14 ("The federal government moved . . . to wipe from its computer systems any software made by a prominent Russian cybersecurity firm, Kaspersky Lab, that is being investigated by the F.B.I. for possible links to Russian security services."); Shirley Zhao, Scott Moritz & Thomas Seal, *Forget 5G, the U.S. and China Are Already Fighting for 6G Dominance*, BLOOMBERG (Feb. 8, 2021), https://www.bloomberg.com/news/features/2021-02-08/forget-5g-the-u-s-and-china-are-already-fighting-for-6g-dominance [https://perma.cc/PW8P-LYYX] (discussing the race between the United States and China to develop 6G technology).

[89] 50 U.S.C. § 4565(a)(4)(B)(iii)(I)–(III), (a)(5), (a)(6).

[90] *See* Tarbert, *supra* note 15, at 1495 (discussing how dual-use technology complicates national security and commercial decisions).

[91] *Critical Infrastructure Sectors*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/critical-infrastructure-sectors [https://perma.cc/D3HU-BUVY] (Oct. 21, 2020).

[92] *See Fortune 500*, FORTUNE, https://fortune.com/fortune500/2021/search/ [https://perma.cc/Y8DF-DCFY] (highlighting the breadth and diversity of large American businesses).

traded companies and used by civilians and the military.[93] Furthermore, some private companies are nationally significant in warfare because they serve like modern mercenaries for their home state as well as foreign states. For example, in 2021, it was reported that a private Israeli company provided critical spyware to allow countries to hack into the systems and phones of their adversaries and critics.[94]

Acts of aggression against any one of these businesses could have serious adverse effects on the military, economy, and general welfare of a country. For instance, imagine if a terrorist organization disabled all the leading broadband Internet service providers and the cellphone services of an entire nation, causing massive disruptions of government, banking, and commercial activities. This is not too far-fetched of a scenario. In 2007, banks and media companies in Estonia were ambushed by a massive cyberattack attributed to Russia that led to unrest in the streets and a nearly devasting standstill of economic activity in much of the country for days.[95] Similarly, in 2017, major businesses in Ukraine were subjected to a major, crippling cyberattack attributed to Russia that then rippled through businesses around the world.[96]

4. Politically Connected Businesses

Politically connected businesses represent another critical category of modern business warfare targets. These businesses are singled out because of their ties to leading political figures and stakeholders, yet they do not fall squarely into the other categories. Politically connected businesses could be attractive for adversaries seeking targets to attack, or entities to use and manipulate as vehicles to sow discord in a competitor's country. A prime example of this category is a business affiliated with former President Donald Trump. Although a Trump-affiliated hotel or Trump Tower may not be a high-value company relative to large, publicly-traded companies, a state-owned enterprise, or a nationally significant business like a major energy company, the fact that it is affiliated so closely with the former President's family makes it an alluring target for U.S. adversaries, requiring a great deal of security, protection, and scrutiny.[97] Among

[93] *See* NICK TURSE, THE COMPLEX: HOW THE MILITARY INVADES OUR EVERYDAY LIVES 5–15 (2008) (highlighting the pervasiveness of private business ties with the U.S. military).

[94] Mark Mazzetti, Adam Goldman, Ronen Bergman & Nicole Perlroth, *In New Age of Digital Warfare, Spies for Any Nation's Budget*, N.Y. TIMES, Mar. 22, 2019, at A1.

[95] Mark Landler & John Markoff, *Digital Fears Emerge After Data Siege in Estonia*, N.Y. TIMES (May 29, 2007), https://www.nytimes.com/2007/05/29/technology/29estonia.html [https://perma.cc/Q63N-BZNH].

[96] Nicole Perlroth, Mark Scott & Sheera Frenkel, *A Cyberattack Hits Ukraine, Then Spreads*, N.Y. TIMES, June 28, 2017, at A1.

[97] *See, e.g.*, Nicholas Fandos, *Budget Deal Allots $120 Million More for First Family's Security*, N.Y. TIMES, May 2, 2017, at A18 (describing the added security needed for protection of former Pres-

American politicians, former President Trump was more the exception than the rule when it came to owning or being affiliated with highly visible businesses during his time in office or after leaving office.[98] That said, in many countries, the political elites are often the business elites as well, possessing significant wealth and economic capital.[99] For instance, the immediate and extended family members of the most senior government officials in China are often also some of the wealthiest and most powerful businesspeople in the country.[100] As such, an adversary could inflict damage on a country by attacking a politically connected business or use it as a means to funnel money into a country to curry favor with certain members of the political elite.

C. The Weapons

The weapons of business warfare are as diverse as the tools of business.[101] The public and private mechanisms that fuel commerce, innovation, and economic growth can also be used to attack and cripple adversaries. The weapons of business warfare can be bifurcated into two broad categories: (1) analog weapons and (2) cyberweapons.[102] Analog weapons include state policy actions like targeted rules, economic sanctions, banking restrictions, and anti-

---

ident Trump's properties); Reuters, *It Cost New York City $24 Million to Secure Trump Tower From Election to Inauguration*, FORTUNE (Feb. 22, 2017), https://fortune.com/2017/02/22/trump-tower-security-costs-taxpayer/ [https://perma.cc/GQW4-CB95] (discussing the cost to New York City of protecting Trump Tower).

[98] *See* Dan Alexander, *These Are the 25 Businesses Quietly Paying Trump $115 Million Each Year*, FORBES (Oct. 28, 2020), https://www.forbes.com/sites/danalexander/2020/10/28/these-are-the-25-companies-quietly-paying-trump-115-million-each-year [https://perma.cc/S78X-WFMK] (documenting various businesses owned by President Trump); Matthew Goldstein, *Trading Surge, Now Scrutinized, Preceded Trump's SPAC Deal*, N.Y. TIMES, Dec. 10, 2021, at B8 (reporting on a post-presidency digital media business venture of former President Trump); Anita Kumar, *How Trump Fused His Business Empire to the Presidency*, POLITICO (Jan. 20, 2020), https://www.politico.com/news/2020/01/20/trump-businesses-empire-tied-presidency-100496 [https://perma.cc/H5CQ-WSVD] (discussing the business ties of President Trump).

[99] *See, e.g.*, Rick Gladstone, *Pandora Papers: A Money Bomb with Political Ripples*, N.Y. TIMES, https://www.nytimes.com/2021/10/04/world/pandora-papers.html [https://perma.cc/A9D2-G8K7] (Oct. 8, 2021) (reporting the hidden economic wealth of some political leaders from around the world).

[100] *See, e.g.*, Alexandra Stevenson & Michael Forsythe, *Lavish Homes Tie China Elite to Hong Kong*, N.Y. TIMES, Aug. 13, 2020, at A1 (reviewing the connections between Chinese political elite and Hong Kong); Michael Forsythe, Chris Buckley & Jonathan Ansfield, *Investigating Family's Wealth, China's Leader Signals a Change*, N.Y. TIMES, Apr. 20, 2014, at A1 (discussing the wealth of China's political elite); David Barboza, *Billions Amassed in the Shadows by the Family of China's Premier*, N.Y. TIMES, Oct. 26, 2012, at A1 (same); David Barboza & Sharon LaFraniere, *China 'Princelings' Using Family Ties to Gain Riches*, N.Y. TIMES, May 18, 2012, at A1 (same).

[101] *See* Lin, *supra* note 14, at 1399 (introducing the concept of financial weapons and discussing analog weapons and cyberweapons).

[102] *Id.*

money laundering regulations.[103] Cyberweapons include distributed denial-of-service attacks, data manipulation, destructive intrusions, ransomware, and other nefarious technological actions.[104] During conflict, business warfare often involves the concerted use of both analog and cyberweapons.

1. Analog Weapons

Analog weapons of business warfare consist of state policy tools to weaken an adversary by restricting its access to the global financial system and targeting specific businesses and industries. Although such state policy tools have long been part of a nation's geopolitical arsenal, their use has arguably grown more prevalent and creative.[105]

Analog weapons have long been a part of global conflict.[106] Ancient Greek and Roman empires, for example, used financial and economic policies to cripple their adversaries.[107] In the early years of the American republic, the United States imposed the Embargo Act of 1807 to punish the British Empire during its war with France.[108] During the Cold War, the United States imposed a series of economic sanctions against the Soviet Union and its Communist allies.[109] In the days following the September 11, 2001 attacks 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.[110] Additionally, the G7 nations, through their Financial Action Task Force, adopted several recommendations against terrorist financing.[111]

---

[103] *Id.*

[104] *Id.*

[105] *See infra* notes 105–132 and accompanying text.

[106] *See* GARY CLYDE HUFBAUER, JEFFREY J. SCHOTT, KIMBERLY ANN ELLIOTT & BARBARA OEGG, ECONOMIC SANCTIONS RECONSIDERED 9–17 (3d ed. 2009) (providing a historical overview of economic sanctions).

[107] *See* KERN ALEXANDER, ECONOMIC SANCTIONS: LAW AND 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 had refused to join the Athenian-led Delian League during the Peloponnesian War."); ZARATE, *supra* note 8, at 3 ("The Greek city-states, the Roman Empire, and even the barbarians used sieges and economic deprivation to weaken their enemies.").

[108] Embargo Act of 1807, ch. 5, 2 Stat. 451 (repealed 1809).

[109] *See* Lin, *supra* note 14, at 1400 & n.120 (citing 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)).

[110] *See id.* & n.121 (first citing International Convention for the Suppression of the Financing of Terrorism, Dec. 9, 1999, 2178 U.N.T.S. 38349; and then citing S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001)).

[111] *See id.* & n.122 (citing FIN. ACTION TASK FORCE, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION: THE FATF RECOMMENDATIONS (updated 2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/

In the post-September 11th era, analog weapons of business warfare have grown more prevalent and creative.[112] The United States has effectively used many analog weapons against its adversaries in recent years to block funding streams for terrorist organizations like Al-Qaeda and ISIS.[113] Likewise, it has cut off access to global financial and economic systems to respond to aggressive actions of North Korea, China, Syria, Iran, and Russia.[114] For instance, in 2014, the United States and its allies imposed a series of severe economic sanctions against Russia and several Russian citizens following Russia's annexation of Crimea.[115]

Other influential countries have behaved similarly. Chinese military officials have publicly opined on how best to use weapons of business warfare in

---

pdfs/FATF%20Recommendations%202012.pdf [https://perma.cc/H5QF-JRGZ] (recommending that countries, among other measures, use effective sanctions, institute mutual legal assistance, and criminalize money laundering offenses)).

[112] *See* MICHAEL G. FINDLEY, DANIEL L. NIELSON & J.C. SHARMAN, GLOBAL SHELL GAMES: EXPERIMENTS IN TRANSNATIONAL RELATIONS, CRIME, AND TERRORISM 1–10 (2014) (describing the problem that shell companies impose and approaches to combat them); MARTIN A. WEISS, CONG. RSCH. SERV., RS21902, TERRORIST FINANCING: THE 9/11 COMMISSION RECOMMENDATION 2 (2005) ("Terrorist organizations are increasingly relying on informal methods of money transfer, and regional cells have begun independently generating funds through criminal activity."); U.S. GOV'T ACCOUNTABILITY OFF., GAO–04–163, TERRORIST FINANCING: U.S. AGENCIES SHOULD SYSTEMATICALLY ASSESS TERRORISTS' USE OF ALTERNATIVE FINANCING MECHANISMS 14 (2003) ("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."); Shima Baradaran, Michael Findley, Daniel Nielson & Jason Sharman, *Funding Terror*, 162 U. PA. L. REV. 477, 482 (2014) (discussing the use of shell companies by terrorist organizations); J.W. Verret, *Terrorism Finance, Business Associations, and the "Incorporation Transparency Act*,*"* 70 LA. L. REV. 857, 857–62 (2010) (discussing the post-September 11th 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, 271 (2014), https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1129&context=penn_law_review_online [https://perma.cc/K4YT-F8CZ] (responding to *Funding Terror* and questioning its premise that terrorists are using shell companies).

[113] *See* ZARATE, *supra* note 8, 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."); Julie Hirschfeld Davis, *Following the ISIS Money*, N.Y. TIMES, Oct. 22, 2014, at B1 (describing the Treasury Secretary's role in helping fight ISIS).

[114] *See* Lin, *supra* note 14, at 1401 & n.127 (citing ZARATE, *supra* note 8, at v–ix); *Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists [https://perma.cc/TQ9V-LFLF] (listing individuals blocked that are owned by targeted countries) (Dec. 2, 2021); Annie Lowrey, *Aiming Financial Weapons from Treasury War Room*, N.Y. TIMES, June 4, 2014, at B1 (detailing Treasury Department's role in targeting countries through financial warfare).

[115] *See* Lin, *supra* note 14, at 1402 & n.133 (citing Peter Baker, *Obama Signals Support for New U.S. Sanctions to Pressure Russian Economy*, N.Y. TIMES, Dec. 17, 2014, at A14).

international conflicts.[116] Over the last decade plus, China has used embargoes of rare earth minerals that are predominantly mined in China and crucial to electronics, to exert pressure on Europe, Japan, and the United States.[117] Most recently, the United States enacted the Anti-Money Laundering Act of 2020, as part of the National Defense Authorization Act for Fiscal Year 2020, to put into place comprehensive safeguards to prevent financing for rogue regimes and terrorist organizations.[118]

Although analog weapons manifest in a wide variety of ways, they can be organized into two crosscutting categories: (1) general restrictions to the global marketplace[119] and (2) targeted regulation on specific companies and industries.[120]

First, general restrictions to the global marketplace can be an incredibly powerful weapon of business warfare, given the interconnectedness and interdependence of modern finance and commerce.[121] They frequently come in the form of economic sanctions, anti-money laundering prohibitions, and banking restrictions. Well-designed and executed restrictions can isolate a nation-state or organization from the global economic system and render it unable to secure resources for its war efforts and ordinary economic activities.[122]

Although other nations regularly utilize these restrictions as weapons of business warfare, the United States plays a central role. Because of the leading role of the United States in global finance and commerce, it wields incredible analog weapons in this space.[123] This is the case because legitimate financial and business institutions fear the reputational risks of being associated with rogue organizations in the eyes of American regulators, policy-makers, and businesses.[124] In recent conflicts with Russia, Syria, Iran, and North Korea, the

---

[116] *See* QIAO LIANG & WANG XIANGSUI, UNRESTRICTED WARFARE: CHINA'S MASTER PLAN TO DESTROY AMERICA 39–41 (2002) (stating that financial warfare will play a central role in warfare in the future).

[117] *See* Keith Bradsher, *China Said to Widen Its Embargo of Minerals*, N.Y. TIMES, Oct. 20, 2010, at B1.

[118] DAVIS POLK & WARDWELL LLP, THE ANTI-MONEY LAUNDERING ACT OF 2020—KEY TAKEAWAYS 1, 11 (2021), https://alerts.davispolk.com/10/5456/uploads/2021-01-04-the-anti-money-laundering-act-of-2020-key-takeaways.pdf [https://perma.cc/FGF9-VWWM].

[119] *See infra* notes 121–127 and accompanying text.

[120] *See infra* notes 128–132 and accompanying text.

[121] ZARATE, *supra* note 8, at 384–85.

[122] *See id.* at 10 (recounting how the "entire toolkit" deployed by the U.S. Treasury Department against illicit financial actors—including sanctions, regulations, and general economic pressure—"created a virtuous cycle of self-solation" that motivated these rogue entities to retreat out of self-interest); Lin, *supra* note 14, at 1404.

[123] *See* ZARATE, *supra* note 8, at 349 ("The reality was that in the new age of financial pressure and a global financial system, American demands and practices applied globally.").

[124] *See id.* at 2–5; P. EDWARD HALEY, STRATEGIES OF DOMINANCE: THE MISDIRECTION OF U.S. FOREIGN POLICY 5 (2006) ("American primacy gave the United States unprecedented freedom of

United States and its allies imposed strict anti-money laundering regulations as a tactic against its adversaries.[125] Similarly, in America's battles against ISIS, one of the most well-funded terrorist organizations in history, the U.S. Treasury Department's Office of the Comptroller of the Currency was on the front line of this battle by choking off funding for terrorism.[126] ISIS has been estimated to possess in excess of $500 million in assets through ransom, looting, extortion, and its capacity to generate $500 million from oil revenue annually, to fund its reign of terror.[127] Because money is so critical to effectuating any attack or defense, these analog weapons of business warfare designed to cut off financing are just as important in this battle as the traditional weapons of bombs and bullets.

Second, targeted regulations on specific businesses and industries are another major category of analog weapons in business warfare. Unlike the general restrictions to financial and economic markets, these weapons focus on particular foreign businesses and industries. These regulations are designed to punish home countries and advantage the country deploying these policies as weapons. For instance, in 2019, the Trump Administration invoked national security interests to levy an array of targeted sanctions and tariffs against a wide range of businesses and industries in China, Mexico, and Japan.[128] Although the targeting of specific companies in global conflict is not new, it has historically focused on companies directly related to national security, such as defense contractors.

Targeted regulations in modern business warfare are different than other categories of analog weapons because they are more expansive and capture more than companies and industries narrowly associated with national defense. China, for instance, has passed onerous regulations requiring all foreign tech-

---

action and brought coercive diplomacy and economic sanctions into the paradigm with much greater frequency . . . ."); Oona Hathaway & Scott J. Shapiro, *Outcasting: Enforcement in Domestic and International Law*, 121 YALE L.J. 252, 258 (2011) (describing the exclusionary effect of law as "outcasting").

[125] *See* Lin, *supra* note 14, at 1403 & n.142 (citing Lowrey, *supra* note 114).

[126] *See id.* & n.143 (first citing JESSICA STERN & J.M. BERGER, ISIS: THE STATE OF TERROR 46 (2015); then citing Rod Nordland, *Iraq Insurgents Reaping Wealth as They Advance*, N.Y. TIMES, June 21, 2014, at A1; and then citing Press Release, U.S. Dep't of the Treasury, Remarks of Under Secretary for Terrorism and Financial Intelligence David S. Cohen 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 [https://perma.cc/9HEU-6AHE]).

[127] *See id.* & n.144 (first citing Cam Simpson & Matthew Philips, *It's More Than Just Oil*, BLOOMBERG BUSINESSWEEK, Nov. 23, 2015, at 10, 11–12; and then citing Matthew Rosenberg, Nicholas Kulish & Steven Lee Myers, *How ISIS Wrings Cash from Those It Now Controls*, N.Y. TIMES, Nov. 30, 2015, at A1).

[128] *See* Ana Swanson & Paul Mozur, *In Name of Security, Trump Sets Off Economic Wars on Multiple Fronts*, N.Y. TIMES, June 9, 2019 (International), at 8 (discussing former President Trump's economic security moves against foreign nations).

nology companies doing business in China to give the state access to all their Chinese user data in the country.[129] This type of regulation has serious national security implications, as it could provide foreign adversaries with access to critical technology and data. Furthermore, such regulatory weapons attempt to overtly harm the economic interests of adversaries by constructively or explicitly banning them from operating in the country. China, for instance, explicitly bans Facebook, Google, and Twitter from operating within its borders.[130] China has also been reported as a leading aggressor in misappropriating intellectual property from prominent American technology companies like Apple and Google.[131] Similarly, Russia requires that technology equipment sold into the country be preinstalled with software that allows the state to track its users and disseminate information.[132]

In sum, the analog weapons of business warfare are state policies and regulations that are utilized to cripple and defeat an adversary by restricting general access to the global financial system and sabotaging specific businesses and industries. These weapons have been used more prevalently and creatively as nations combat each other in a shared global financial and economic marketspace.

2. Cyberweapons

In addition to analog weapons, modern business warfare also involves cyberweapons because of the highly intermediated electronic networks that serve as the informational infrastructure of commerce and geopolitics.[133] Increasingly, cyberweapons are becoming a preferred tool of warfare between nation-states.[134] The volume and variety of cyberattacks on business institu-

---

[129] Sui-Lee Wee, *China's New Cybersecurity Law Leaves Foreign Companies Guessing*, N.Y. TIMES, June 1, 2017, at B3.

[130] Kim Lyons, *Google, Facebook, and Twitter Halt Government Data Requests After New Hong Kong Security Law*, THE VERGE (July 6, 2020), https://www.theverge.com/2020/7/6/21314900/google-facebook-twitter-hong-kong-government-data-china [https://perma.cc/RZ7C-49WP].

[131] SANGER, *supra* note 15, at 120–25.

[132] *See* Mark Scott, *Russia Prepares to Block LinkedIn*, N.Y. TIMES, Nov. 11, 2016, at B1 (reporting that Russia blocked access to LinkedIn for its violation of Russian laws regarding personal digital data of Russian citizens); Madeline Roache, *How Russia Is Stepping Up Its Campaign to Control the Internet*, TIME (Apr. 1, 2021), https://time.com/5951834/russia-control-internet/ [https://web.archive.org/web/20211119160317/https://time.com/5951834/russia-control-internet/] (describing new Russian laws requiring Internet Service Providers to install Deep Packet Inspection equipment that allows Russia to block content and reroute Internet traffic).

[133] *See* Lin, *supra* note 14, at 1405 (introducing the idea of cyber weapons); SANGER, *supra* note 15, at 300–05; Tom C.W. Lin, *Infinite Financial Intermediation*, 50 WAKE FOREST L. REV. 643, 645–53 (2015) (discussing the intermediated networks underlying the global financial system).

[134] *See generally* NICOLE PERLROTH, THIS IS HOW THEY TELL ME THE WORLD ENDS: THE CYBERWEAPONS ARMS RACE (2021) (noting the rise of cyberweapons and cyberattacks).

tions, like all cyberattacks, increases annually.[135] As such, many countries, including the United States, have dedicated intelligence and military divisions focused solely on cyberattacks.[136]

In modern warfare and global conflicts, the first shots of battle are often fired in cyberspace at business targets.[137] In an early incident of cyberweapons being used in warfare, during a geopolitical dispute in 2007, Russia launched a nationwide cyberattack on Estonia's cyber infrastructure that temporarily crippled the country's financial system and economy.[138] In 2012, a terrorist organization that some believed had ties to Iran, called the Izz ad-Din al-Qassam Cyber Fighters, launched a sophisticated cyberattack on six major American banks and the New York Stock Exchange that rendered those institutions temporarily inaccessible to their customers and clients.[139] In 2013, Iran unleashed a round of persistent denial-of-service attacks on several major American banks in retaliation for American sanctions and policies in the Middle East.[140] In 2015, it was reported 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 at the time amounted to what is believed to be the most pervasive cyberattack on the American government's cyber infrastructure.[141] A few years later, China would also attack credit reporting giant Equifax, to steal the personal information of millions of Americans.[142] And again in 2021, China was accused of hacking Microsoft email systems that leading businesses, governments, and militaries around the world were using.[143] These cyberattacks and others, in aggregate,

---

[135] *See* Lin, *supra* note 14, at 1405–06, 1406 n.156 (citing FIN. INDUS. REGUL. AUTH., REPORT ON CYBERSECURITY PRACTICES 1 (2015), https://www.finra.org/sites/default/files/2020-07/2015-report-on-cybersecurity-practices.pdf [https://perma.cc/9K7E-SSVR]).

[136] 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 [https://perma.cc/FUY5-637C].

[137] *See* Lin, *supra* note 14, at 1406.

[138] *See* Landler & Markoff, *supra* note 95 (recounting the cyberattack on Estonia).

[139] *See* Lin, *supra* note 14, at 1407 & n.168 (citing Nicole Perlroth, *Attacks on 6 Banks Frustrate Customers*, N.Y. TIMES, Oct. 1, 2012, at B1 (describing the cyberattack on American banks and its effects)).

[140] *See, e.g.*, Nicole Perlroth & Quentin Hardy, *Bank Hacks Were Work of Iranians, Officials Say*, N.Y. TIMES, Jan. 9, 2013, at B1 (documenting the effects of serious cyberattacks on American banks).

[141] *See* Lin, *supra* note 14, at 1410 & n.183 (citing Julie Hirschfeld Davis, *Hacking Exposed 21 Million in U.S., Government Says*, N.Y. TIMES, July 10, 2015, at A1).

[142] Brian Barrett, *How 4 Chinese Hackers Allegedly Took Down Equifax*, WIRED (Feb. 10, 2020), https://www.wired.com/story/equifax-hack-china/ [https://perma.cc/U4Z5-LJAH] (revealing that the Equifax hack exposed the personal information of 143 million U.S. citizens).

[143] Zolan Kanno-Youngs & David E. Sanger, *U.S. and Key Allies Accuse China in String of Global Cyberattacks*, N.Y. TIMES, July 20, 2021, at A1.

gave the Chinese government an enormous treasure trove of sensitive data on millions of Americans and thousands of American businesses.

The tactics involving cyberweapons in business warfare are multivariate. Common tactics involve distributed denial-of-service (DDoS) attacks, data manipulation or semantic attacks, destructive intrusion hacks, and ransomware.[144] First, DDoS attacks are cyber incursions that attempt to disrupt and suspend the service of an online host for its users.[145] DDoS attacks inundate a site or server with fraudulent and malicious activity until it ceases to function properly, or at all.[146] In 2015, it was reported that China possessed cyberweapons that could intercept and redirect a tsunami of Internet traffic to sites that it wanted to shut down.[147]

Second, data manipulation hacks or semantic attacks describe cyber aggressions that plunder or maliciously alter data towards destructive ends.[148] Such attacks can be designed to disrupt trading markets, steal intellectual property, and embezzle funds from the private businesses of adversary states.[149] These attacks can cause serious economic and psychological damage because investors and consumers lose faith in businesses' abilities to safeguard the integrity of markets.[150]

Third, destructive intrusion hacks are used to gain valuable intelligence or destroy valuable physical assets by gaining unauthorized access into an adversary's information systems.[151] In 2011, the United States and Israel reportedly

---

[144] *See* Lin, *supra* note 14, at 1407 (explaining the common cyberweapons currently used).

[145] *See id.* & n.166 (citing Hathaway et al., *supra* note 15, at 837 (describing DDoS attacks as "coordinated botnets—collections of thousands of 'zombie' computers hijacked by insidious viruses—[that] overwhelm servers by systematically visiting designated websites")).

[146] *Id.* at 1407; *see* Hathaway et al., *supra* note 15, at 837.

[147] *See* Lin, *supra* note 14, at 1408 & n.170 (citing Nicole Perlroth, *Chinese Tool Is Suspected in Web Attack*, N.Y. TIMES, Apr. 11, 2015, at B1).

[148] *See id.* & n.171 (first citing MARTIN C. LIBICKI, WHAT IS INFORMATION WARFARE?, at 77 (1995) (describing a semantic attack); then citing Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1042 (2007) (questioning how to label cyberattacks); and then citing Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SEC. L. & POL'Y 63, 67 (2010) (discussing the effects of cyberattacks on data integrity and authenticity)).

[149] *See* Reuters, *China Theft of Technology Is Biggest Law Enforcement Threat to US, FBI Says*, THE GUARDIAN (Feb. 6, 2020), https://www.theguardian.com/world/2020/feb/06/china-technology-theft-fbi-biggest-threat [https://perma.cc/X5RM-AWHG] (documenting the current and future damage to the United States by Chinese cybertheft).

[150] *See* NAT'L BUREAU OF ASIAN RSCH., THE IP COMMISSION REPORT: THE REPORT OF THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY 1–7 (2013), https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report.pdf [https://perma.cc/PG4Z-6DXG] (reporting on the grave effects that intellectual property theft has on the United States).

[151] *See* Press Release, U.S. Dep't of the Treasury, Remarks of Secretary Jacob J. Lew at the 2014 Delivering Alpha Conference Hosted by CNBC and Institutional Investor (July 16, 2014), https://www.treasury.gov/press-center/press-releases/Pages/jl2570.aspx [https://perma.cc/9SVC-LF4H]; Lin,

released Stuxnet, a computer virus super-worm, deemed by some at the time as "the most sophisticated cyberweapon ever deployed," to destroy an Iranian nuclear weapons facility.[152] Stuxnet destroyed the centrifuges in the nuclear facility by gaining illegal access into its computer system and clandestinely reprogramming the centrifuges to overwork until destruction.[153] More recently, in 2021, it was reported that numerous nation-states used spyware developed by a private Israeli company to hack into the systems of foreign adversaries, opposition activists, and critical journalists.[154]

Fourth, ransomware attacks are cyber-aggressions to lock a party out of their own files and systems until a ransom is paid.[155] Ransomware attacks can target individual files, standalone computers, or entire networks and systems.[156] Such attacks can be highly lucrative for bad actors and cause serious economic disruptions to businesses and states.[157] In 2017, the WannaCry ransomware attack, widely attributed to North Korea, caused significant disruptions to businesses and government entities around the world when it infected numerous computer systems, including the National Health Service of the United Kingdom.[158] Over time, ransomware attacks have grown more prevalent and pernicious.[159] In 2021 alone, one of the largest pipelines in the United

---

supra note 15, at 1306–07; Nicole Perlroth & David E. Sanger, *Cyberattacks Seem Meant to Destroy, Not Just Disrupt*, N.Y. TIMES, Mar. 29, 2013, at B1; John Seabrook, *Network Insecurity: Are We Losing the Battle Against Cyber Crime?*, NEW YORKER (May 13, 2013), https://www.newyorker.com/magazine/2013/05/20/network-insecurity [https://perma.cc/NY9J-R2HT].

[152] *See* Lin, *supra* note 14, at 1408 & n.178 (first quoting William J. Broad, John Markoff & David E. Sanger, *Israel Tests Called Crucial in Iran Nuclear Setback*, N.Y. TIMES, Jan. 16, 2011, at A1; then citing KIM ZETTER, COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON 52–70 (2014)).

[153] *See id.* & n.179 (citing Broad et al., *supra* note 152).

[154] *See* Ronen Bergman & Patrick Kingsley, *Spyware Report Brings Scrutiny to Israeli Firm*, N.Y. TIMES, July 19, 2021, at A1; Dana Priest, Craig Timberg & Souad Mekhennet, *Private Israeli Spyware Used to Hack Cellphones of Journalists, Activists Worldwide*, WASH. POST, https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/ [https://perma.cc/2P5H-G9BR] (July 18, 2021).

[155] *See* MULTI-STATE INFO. SHARING & ANALYSIS CTR., RANSOMWARE GUIDE: SEPTEMBER 2020, at 2 (2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf [https://perma.cc/Y3XT-5HKE].

[156] Kim Zetter, *What Is Ransomware? A Guide to the Global Cyberattack's Scary Method*, WIRED (May 14, 2017), https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/ [https://perma.cc/6AVW-S369].

[157] *Id.* (estimating, conservatively, that ransomware attacks extort at least $5 million each year).

[158] *See* David E. Sanger, *U.S. Accuses North Korea of Cyberattack on British Health System*, N.Y. TIMES, Dec. 19, 2017, at A18; Josephine Wolff, Opinion, *How Ransomware Puts Your Hospital at Risk*, N.Y. TIMES, Oct. 19, 2020, at A25 (estimating that the WannaCry malware cost the hospital around $118 million).

[159] *See* PERLROTH, *supra* note 134, at 333–40; Lynsey Jeffery & Vignesh Ramachandran, *Why Ransomware Attacks Are on the Rise—and What Can Be Done to Stop Them*, PBS NEWSHOUR (July

States, Colonial Pipeline, and one of the largest meat processors in the world, JBS, were both attacked with ransomware attributed to Russian hackers.[160] In both incidents, national and global supply chains for energy and food experienced serious disruptions, and both companies ultimately paid millions of dollars each to their attackers to regain control of their systems.[161]

Although the tactics of cyberweapons on business warfare may be multivariate, the overarching singular goal is to weaken adversaries by damaging their public institutions and private businesses. American businesses and interests are particularly vulnerable to cyberweapons in business warfare because of their heavy reliance on high-tech informational networks.[162] Numerous business surveys and studies highlight how cyberattacks are consistently one of the main concerns of American business leaders.[163] In recent years, reports found that American companies were subjected to over 15,000 cyberattacks annually, and those threats are growing and costing the economy billions of dollars every year.[164] To be clear, while cyberattacks are commonplace in business warfare, it should be noted that not all cyberattacks are related to businesses warfare. Many cyberattacks against businesses are purely criminal in nature by bad actors who seek illicit gains without any national security implications.

In response to the rising and evolving threats posed by cyberweapons, the federal government and private businesses have both responded with greater efforts and investments to combat these threats.[165] Both the federal government

---

8, 2021), https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them [https://perma.cc/BT98-TF32].

[160] *See* David E. Sanger, Clifford Krauss & Nicole Perlroth, *Major Pipeline Forced to Close by Cyberattack*, N.Y. TIMES, May 9, 2021, at A1; Rebecca Robbins, *Meat Processor Paid Hackers a Ransom Worth $11 Million*, N.Y. TIMES, June 10, 2021, at A15; Editorial, *The Plague of Ransomware*, N.Y. TIMES, Aug. 1, 2021 (Sunday Review), at 8.

[161] Editorial, *supra* note 160.

[162] *See* Waxman, *supra* note 18, 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."); DEP'T OF DEF., THE DEPARTMENT OF DEFENSE CYBER STRATEGY 2 (2015), https://www.hsdl.org/?view&did=764848 [https://perma.cc/QKC4-MJ3X] ("A disruptive, manipulative, or 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."); Nicole Perlroth & Elizabeth A. Harris, *Cyberattack Insurance a Challenge for Business*, N.Y. TIMES, June 9, 2014, at B1 (describing the increase in insurance for cyberattacks).

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

[164] *See* Lev Grossman, *The Code War*, TIME, July 21, 2014, at 18, 20 (noting that "the average American company fielded a total of 16,856 cyberattacks in 2013"); Devon Hourihan, *15 Alarming Cyber Security Facts and Stats*, CYBINT (Dec. 23, 2020), https://www.cybintsolutions.com/cyber-security-facts-stats/ [https://perma.cc/79YL-WLVW].

[165] *See, e.g.*, Hathaway et al., *supra* note 15, at 874–77 (identifying legal and policy challenges presented by cyberattacks); MARK BOWDEN, WORM: THE FIRST DIGITAL WORLD WAR 48–53 (2011)

and private businesses have reportedly taken innovative and controversial steps, like participating in zero-day markets for software vulnerabilities, whereby they purchase vulnerabilities in software for fixing or exploitation; or the Central Intelligence Agency establishing its own venture capital fund, In-Q-Tel, to support the development of intelligence-related technologies in the private sector.[166]

For the avoidance of doubt, the United States does not only play defense on cyber warfare; it is also one of the most capable users of cyberweapons. Publicly released, classified information suggested that the United States initiated over two hundred offensive cyberattacks in 2011, many with important military and economic implications, against China, Iran, Russia, and North Korea.[167] A few years later, the United States reportedly embedded "surveillance and sabotage tools" in targeted computer systems of its adversaries in Iran, Russia, Pakistan, China, Afghanistan, and other countries.[168] More recently, in 2020, the United States initiated a massive cyber offensive against the world's largest botnet reportedly affiliated with Russia in advance of the 2020 election, to prevent it from disrupting the American economy and presidential race.[169]

In sum, modern business warfare involves not only the use of traditional, analog weapons, but also the use of powerful, tactical cyberweapons. These weapons could cause massive financial chaos, destroy profitable businesses, and create an economic crisis, to say nothing of the psychological and emo-

---

(describing challenges in creating a cybersecurity defense system); Christopher M. Matthews, *Cybertheft Victims Itchy to Retaliate*, WALL ST. J., June 3, 2013, at B6 (exploring the option of cybertheft victims retaliating); Chris Strohm, Eric Engleman & Dave Michaels, *Cyber Attack? What Cyber Attack?*, BLOOMBERG BUSINESSWEEK, Apr. 15, 2013, at 40, 40 (reporting on the reluctance of companies to disclose cyberattacks); Michael Joseph Gross, *Enter the Cyber-Dragon*, VANITY FAIR, Sept. 2011, at 220, 222 ("Because virtual attacks can be routed through computer servers anywhere in the world, it is almost impossible to attribute any hack with total certainty."); Sarah Gordon & Richard Ford, *On the Definition and Classification of Cybercrime*, 2 J. COMPUT. 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.").

[166] *See, e.g.*, LILLIAN ABLON & ANDY BOGART, ZERO DAYS, THOUSANDS OF NIGHTS: THE LIFE AND TIMES OF ZERO-DAY VULNERABILITIES AND THEIR EXPLOITS 22–26 (2017) (discussing zero-day markets); Jon D. Michaels, *The (Willingly) Fettered Executive: Presidential Spinoffs in National Security Domains and Beyond*, 97 VA. L. REV. 801, 805–07 (2011) (discussing In-Q-Tel).

[167] *See* Lin, *supra* note 14, at 1406 & n.158 (first citing Barton Gellman & Ellen Nakashima, *'Black Budget' Details a War in Cyberspace*, WASH. POST, Aug. 31, 2013, at A1; then citing Michael Riley, *How the U.S. Government Hacks the World*, BLOOMBERG BUSINESSWEEK, May 27, 2013, at 35, 35–37).

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

[169] Ellen Nakashima, *Cyber Command Has Sought to Disrupt the World's Largest Botnet, Hoping to Reduce Its Potential Impact on the Election*, WASH. POST (Oct. 9, 2020), https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html [https://perma.cc/2DJS-PNSU].

tional toll it can exact on its victim countries and companies.[170] As more businesses adopt advanced technologies like artificial intelligence, blockchains, and other new innovations, the threats of cyberweapons in business warfare will only loom larger.[171]

II. Recent Episodes

The threats of business warfare are not merely theoretical or academic in nature. Countries and companies, wittingly or unwittingly, are on the frontlines of this new theater of conflict on a daily basis. Recent episodes involving Russia, Iran, China, and the United States highlight variations and manifestations of business warfare and its geopolitical implications on law, business, and society. Section A of this Part first reviews the hacks perpetrated by Russia during the COVID-19 pandemic.[172] Section B then examines the attacks orchestrated by Iran against both Saudi Arabia and the United States.[173] Finally, Section C analyzes the contentious history of cyberattacks between China and the United States.[174]

A. Russia and the Pandemic Hacks

In 2020, as the world paused much of its regular activities to confront a global pandemic, Russia continued its decades-long post-Cold War assault on the United States and other Western democracies.[175] Rather than engage in traditional armed conflict via proxies, like it did during the Cold War, Russia's preferred methods of engagement now appear to be using cyberattacks and high-tech misinformation campaigns to steal, damage, and disrupt its adver-

---

[170] P.W. Singer & Emerson T. Brooking, LikeWar: The Weaponization of Social Media 20–23 (2018) (describing how the Internet has become a war field).

[171] *See* William Magnuson, Blockchain Democracy: Technology, Law and the Rule of the Crowd 95–111 (2020) (discussing the crimes and misconduct that could be perpetuated using blockchain technology); Brad Smith & Carole Ann Browne, Tools and Weapons: The Promise and the Peril of the Digital Age 69–76 (2019) (highlighting cybersecurity threats posed by emerging technologies); Tom C.W. Lin, *Artificial Intelligence, Finance, and the Law*, 88 Fordham L. Rev. 531, 532–35 (2019) (noting the growing use of artificial intelligence systems in finance).

[172] *See infra* notes 175–192 and accompanying text.

[173] *See infra* notes 193–205 and accompanying text.

[174] *See infra* notes 206–238 and accompanying text.

[175] *See* Brose, *supra* note 15, at 25–27 (discussing Russia's post-Cold War posture towards the United States and its neighbors in Europe); *see, e.g.*, Bill Chappell, Greg Myre & Laurel Wamsley, *What We Know About Russia's Alleged Hack of the U.S. Government and Tech Companies*, NPR (Dec. 21, 2020), https://www.npr.org/2020/12/15/946776718/u-s-scrambles-to-understand-major-computer-hack-but-says-little [https://perma.cc/L5V6-CDXZ] (describing the SolarWinds cyberattack on the U.S. government and private American companies); *Norway Blames Russia for Cyber-Attack on Parliament*, BBC News (Oct. 13, 2020), https://www.bbc.com/news/world-europe-54518106 [https://perma.cc/KJ8D-W67D] (noting that Norway blames Russia for a cyberattack on its government).

saries.[176] Most notably, in 2016, Russia used cyberweapons to influence the outcome of the U.S. presidential election through persistent hacking, misinformation, and data manipulation campaigns.[177] The targets of these latest cyberattacks are government entities, but more and more they are also private business entities. In 2020, Russia or Russian-affiliated actors reportedly launched at least two major cyberattacks during the global pandemic.[178]

First, Russia launched cyberattacks on American and British pharmaceutical companies working on the coronavirus vaccines with the hope of plundering research to produce a vaccine for Russia, which had lost over 186,000 citizens to the pandemic by the end of 2020.[179] In July 2020, the U.S. National Security Agency and its counterparts in the United Kingdom and Canada discovered and accused Russia of trying to steal intellectual property and scientific information from private and public institutions working on a coronavirus vaccine.[180] The United States, Canada, and the United Kingdom attributed the attack to a unit affiliated with Russian intelligence known as APT29, or Cozy Bear.[181] This was the same group linked to the attacks on the Democratic Party and the American electoral process in 2016.[182] At the time of the disclosure in July 2020, American and British companies, Pfizer, Moderna, and AstraZeneca, were at the forefront of developing an effective COVID-19 vaccine.[183]

Second, in December 2020, it was revealed that Russia had engaged in an unprecedented cyberattack on the highest level of American government and American business.[184] Using a "tainted software update" by SolarWinds, an American software company, hackers associated with the top Russian intelligence agency (S.V.R.) gained access into the servers of almost every agency in the federal government, including the Defense, Homeland Security, State, and

---

[176] JASPER, *supra* note 32, at 15.

[177] *Id.* at 77–82.

[178] Julian E. Barnes, *Russians Accused of a Plot to Steal Vaccine Research*, N.Y. TIMES, July 17, 2020, at A1 (finding that Russian hackers attempted to steal vaccine research and data).

[179] *See id.* (discussing Russian cyberattacks on pharmaceutical companies working on coronavirus vaccines); Kim Lyons, *Microsoft Says Hackers from Russia and North Korea Attacked COVID-19 Vaccine Makers*, THE VERGE (Nov. 14, 2020), https://www.theverge.com/2020/11/14/21565136/microsoft-hackers-russia-north-korea-attacked-covid-19-vaccine-coronavirus [https://perma.cc/CEW7-NNFS] (same); *see also* Andrew Higgins, *New Data Triples Russia's Death Toll*, N.Y. TIMES, Dec. 30, 2020, at A5 (discussing Russia's death toll due to the coronavirus pandemic).

[180] Barnes, *supra* note 178.

[181] *Id.*

[182] *Id.*

[183] *See* Carl Zimmer, Jonathan Corum & Sui-Lee Wee, *Coronavirus Vaccine Tracker*, N.Y. TIMES, https://www.nytimes.com/interactive/2020/science/coronavirus-vaccine-tracker.html [https://perma.cc/RY6B-E458].

[184] David E. Sanger, Nicole Perlroth & Eric Schmitt, *Agencies Race to Assess Damage After Being Hacked by Russia*, N.Y. TIMES, Dec. 15, 2020, at A1.

Treasury Departments.[185] The hackers also breached a number of large American corporations, many of which used SolarWinds software.[186] This Russian cyberattack has been viewed by many as one of the largest and most consequential intelligence and defense failures in American history.[187] U.S. Senator Dick Durbin called the attack "virtually a declaration of war."[188] Then President-elect Joe Biden called for stronger cyber defenses as well as preemptive offensive action: "A good defense isn't enough; we need to disrupt and deter our adversaries from undertaking significant cyberattacks in the first place."[189] Brad Smith, the President of Microsoft, lamented the wide-scale attack on businesses as well as government agencies, calling for "a clear set of rules that put certain techniques off limits."[190] What Mr. Smith recognized, perhaps earlier than many of his political and business counterparts, was the rising threats of business warfare where countries target businesses without any clear international norms or rules to govern their aggression.[191]

These two cases involving Russia highlight how diminished, yet powerful Cold War adversaries use business warfare to continue to wreak havoc on the global stage against a superior United States, with grave economic, political, and national security consequences.[192]

B. Iran, Saudi Aramco, and American Finance

Iran has had a long, complicated, conflict-filled relationship with the United States and many of its regional neighbors.[193] Centuries and decades-

---

[185] *Id.*

[186] *Id.*; David E. Sanger & Nicole Perlroth, *Range of Tools in a Vast Hack Elevates Fears*, N.Y. TIMES, Dec. 18, 2020, at A1.

[187] David E. Sanger, Nicole Perlroth & Julian E. Barnes, *U.S. Cyberdefenses Cost Billions, but Russian Hackers Eluded Them*, N.Y. TIMES, Dec. 17, 2020, at A20.

[188] Jan Wolfe & Brendan Pierson, *Explainer—U.S. Government Hack: Espionage or Act of War?*, REUTERS (Dec. 19, 2020), https://www.reuters.com/article/global-cyber-legal/explainer-u-s-government-hack-espionage-or-act-of-war-idUSKBN28T0HH [https://perma.cc/3T6A-Y7C3] (stating that the hack would not be considered an act of war under current international law, but rather, that it was an act of espionage).

[189] Sanger & Perlroth, *supra* note 186 ("I will not stand idly by in the face of cyberassaults on our nation." (quoting Joe Biden, President-elect)).

[190] *Id.*

[191] *Id.* ("One of the things that needs to be off limits is a broad supply chain attack that creates a vulnerability for the world that other forms of traditional espionage do not." (quoting Brad Smith, President, Microsoft)).

[192] *See* TIM WEINER, THE FOLLY AND THE GLORY: AMERICA, RUSSIA, AND POLITICAL WARFARE, 1945–2020, at 1–3, 233–37 (2020) (discussing how Russia continues to antagonize the United States in unconventional ways decades after losing the Cold War).

[193] *See* KIM GHATTAS, BLACK WAVE: SAUDI ARABIA, IRAN, AND THE FORTY-YEAR RIVALRY THAT UNRAVELED CULTURE, RELIGION, AND COLLECTIVE MEMORY IN THE MIDDLE EAST 2–4 (2020) (reviewing the relationship between Iran and Saudi Arabia); DAVID CRIST, THE TWILIGHT

long disputes in the Middle East have resulted in numerous skirmishes, wars, assassinations, bombings, terrorist acts, and other forms of aggression between and amongst countries.[194] Not surprisingly, with the emergence of business warfare, Iran has also pursued this evolving form of hostility against its adversaries. Two episodes, one involving Saudi Arabia, and another involving the United States, highlight Iran's use of business warfare against its adversaries in global conflicts.[195]

With regards to Saudi Arabia, on September 14, 2019, drones and missiles unleashed an attack on the state-owned company Saudi Aramco's facilities in Abqaiq and Khurais.[196] The United States, Saudi Arabia, and many of its allies later attributed the attacks to Iran, even though the Houthi movement of Yemen claimed sole responsibility.[197] The attacks caused major fires, damage, and destruction at both facilities, forcing the company to shut down production at both sites.[198] Because of the importance of Saudi Arabia to global oil markets, the attack and subsequent shut down ostensibly led to a five percent decline in global oil production and caused global economic disruptions.[199] The attack on state-owned Saudi Aramco was particularly consequential because Saudi Arabia was in the process of taking the company public through what still remains the largest IPO in world history.[200] This attack on Saudi Aramco serves as one of the most aggressive and public cases of modern business warfare.

WAR: THE SECRET HISTORY OF AMERICA'S THIRTY-YEAR CONFLICT WITH IRAN 5–10 (2012) (explaining the complex and conflict-filled relationship between the United States and Iran); JOHN GHAZVINIAN, AMERICA AND IRAN: A HISTORY, 1720 TO THE PRESENT, at xii–xviii (2021) (same).

[194] *See generally* GHATTAS, *supra* note 193, at 2–4 (documenting the disputes in the Middle East).

[195] *See infra* notes 196–200 (describing 2019 attacks on the Saudi Arabian company, Saudi Aramco, that the United States and Saudi Arabia attributed to Iran); *infra* notes 201–205 (describing Iranian attacks from 2011 to 2013 against U.S. finance corporations).

[196] Hubbard et al., *supra* note 10.

[197] *Id.*

[198] *Id.*

[199] Stephen Kalin, Rania El Gamal & Dmitry Zhdannikov, *Attacks on Saudi Oil Facilities Knock Out Half the Kingdom's Supply*, REUTERS (Sept. 13, 2019), https://www.reuters.com/article/us-saudi-aramco-fire/attacks-on-saudi-oil-facilities-knock-out-half-the-kingdoms-supply-idUSKCN1VZ01N [https://perma.cc/KH8G-SZZG]; Laila Kearney, *Oil Jumps Nearly 15% in Record Trading After Attack on Saudi Facilities*, REUTERS (Sept. 15, 2019), https://www.reuters.com/article/us-global-oil/oil-prices-surge-15-after-attack-on-saudi-facilities-hits-global-supply-idUSKBN1W00UG [https://perma.cc/3VC4-8868].

[200] *See* Kate Kelly & Stanley Reed, *A $2 Trillion Wish That the Markets Just Couldn't Grant*, N.Y. TIMES, Dec. 7, 2019, at B1; Aya Batrawy, *Saudi Aramco Stock Gains 10 Percent After It Begins Trading*, PBS NEWSHOUR (Dec. 11, 2019), https://www.pbs.org/newshour/economy/saudi-aramco-stock-gains-10-percent-after-it-begins-trading [https://perma.cc/K47Q-AK8V] (announcing that Saudi Aramco's IPO was the largest in history).

With regard to the United States, between 2011 and 2013, Iran launched a series of sustained cyberattacks on the American financial sector in response to American sanctions.[201] The attack targeted some of the largest financial institutions, including household names like Bank of America, J.P. Morgan, Citigroup, and the New York Stock Exchange.[202] These attacks led to serious business disruptions and denial-of-services throughout the American financial sector and the American economy.[203] The attacks slowed and harmed the flow of funds in the American financial system, which serves as the lifeblood of the American—and global—economies. In announcing charges against Iranians tied to the attacks, the Department of Justice in 2016 observed that "[t]hese were no ordinary crimes, but calculated attacks by groups with ties to Iran's Islamic Revolutionary Guard and designed specifically to harm America and its people."[204] In the years following these audacious cyberattacks on American finance and as tensions remained high between the two countries, Iran would continue to target American businesses as a means to hurt the United States.[205]

In both cases, rather than engage in outright, costly, full-scale traditional wars that it would likely lose against its better-resourced adversaries, Iran engaged in business warfare, using cyberattacks to target valuable businesses in Saudi Arabia and the United States.

---

[201] *See* Perlroth & Hardy, *supra* note 140; Press Release, Dep't of Just. Off. of Pub. Affs., Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector (Mar. 24, 2016), https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged [https://perma.cc/DY4U-GD7R]; Jim Finkle & Rick Rothacker, *Exclusive: Iranian Hackers Target Bank of America, JPMorgan, Citi*, REUTERS (Sept. 21, 2012), https://www.reuters.com/article/us-iran-cyberattacks/exclusive-iranian-hackers-target-bank-of-america-jpmorgan-citi-idUSBRE88K12H20120921 [https://perma.cc/V49J-LQZC].

[202] *See, e.g.*, Perlroth, *supra* note 139 (noting the major financial institutions that were victims of the cyberattacks); Perlroth & Hardy, *supra* note 140 (same).

[203] *See* Perlroth & Hardy, *supra* note 140; *U.S. Charges Iranian Hackers in Wall Street Cyber-Attacks*, AM. BANKER (Mar. 24, 2016), https://www.americanbanker.com/news/us-charges-iranian-hackers-in-wall-street-cyber-attacks [https://perma.cc/8ZGX-6QC4].

[204] Press Release, Dep't of Just. Off. of Pub. Affs., *supra* note 201.

[205] *See* Shannon Bond, *Iran Conflict Could Shift to Cyberspace, Experts Warn*, NPR (Jan. 21, 2020), https://www.npr.org/2020/01/21/797449708/iran-conflict-could-shift-to-cyberspace-experts-warn [https://perma.cc/UYM7-G9NJ]; Eric Geller, *U.S. Calls Out Iranian Hacker Threat with Indictment, Sanctions and Threat Analysis*, POLITICO (Sept. 17, 2020), https://www.politico.com/news/2020/09/17/iran-hacker-threat-indictment-sanctions-417014 [https://perma.cc/F47D-27TG]; Sue Halpern, *Should the U.S. Expect an Iranian Cyberattack?*, NEW YORKER (Jan. 6, 2020), https://www.newyorker.com/tech/annals-of-technology/should-the-us-expect-an-iranian-cyberattack [https://perma.cc/F6PM-4AUB]; *Publicly Reported Iranian Cyber Actions in 2019*, CTR. FOR STRATEGIC & INT'L STUD., https://www.csis.org/programs/technology-policy-program/publicly-reported-iranian-cyber-actions-2019 [https://perma.cc/6FWX-YDEA].

C. China, Huawei, and TikTok

The relationship between the United States and China has grown continuously more contentious over the last decade, as the American superpower confronts the rising power of China on the global stage.[206] Because of economic interdependence, the two countries have engaged in business warfare as they compete for economic supremacy and global dominance, rather than engage one another in traditional, open warfare and armed conflict.[207] This contentious economic engagement is illustrated by two well-publicized episodes from 2020 involving the Chinese technology companies Huawei and TikTok.

In terms of Huawei, in recent years, the United States placed severe restrictions on the Chinese company given its close ties with the Chinese government and allegations of intellectual property theft, espionage, and other misconduct.[208] Based in Shenzhen, China, Huawei is one of the largest technology companies in the world.[209] It is a leading manufacturer of telecommunications equipment and smartphones.[210] After Samsung, it is the second largest producer of smartphones in the world.[211] In 2018, the United States prohibited the federal government and federal contractors from using Huawei equipment for national security reasons.[212] The American intelligence community had long worried about the Chinese government leveraging Huawei equipment to spy and steal from American businesses and government agencies.[213] This restriction meant that most businesses operating in the United States could not use Huawei equipment, given the federal government's far-reaching procurement breadth.[214] In December 2018, the United States ordered the arrest of Huawei's chief financial officer, Meng Wanzhou, in Canada; Ms. Meng is also

---

[206] *See* GRAHAM ALLISON, DESTINED FOR WAR: CAN AMERICA AND CHINA ESCAPE THUCYDIDES'S TRAP?, at vii–x (2017) (describing the rising power of China and its threat to displace the current ruling power, the United States); BROSE, *supra* note 15, at 34–39 (discussing the military threat China poses for the United States); BOB DAVIS & LINGLING WEI, SUPERPOWER SHOWDOWN: HOW THE BATTLE BETWEEN TRUMP AND XI THREATENS A NEW COLD WAR 387–95 (2020) (chronicling the multidecade-long economic competition between China and the United States).

[207] DAVIS & WEI, *supra* note 206, at 360–65.

[208] David McCabe & Raymond Zhong, *U.S. Tightens Restrictions on Huawei's Chip Access*, N.Y. TIMES, Aug. 18, 2020, at B1.

[209] *Who Is Huawei*, HUAWEI, https://www.huawei.com/us/corporate-information [https://perma.cc/37PL-VBG6].

[210] *Id.*

[211] *Id.*

[212] Jacob Kastrenakes, *Trump Signs Bill Banning Government Use of Huawei and ZTE Tech*, THE VERGE (Aug. 13, 2018), https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump [https://perma.cc/U75G-AXZA].

[213] James Vincent, *Don't Use Huawei Phones, Say Heads of FBI, CIA, and NSA*, THE VERGE (Feb. 14, 2018), https://www.theverge.com/2018/2/14/17011246/huawei-phones-safe-us-intelligence-chief-fears [https://perma.cc/J7PD-RWSE].

[214] *See* Kastrenakes, *supra* note 212 (describing the breadth of the ban on Huawei products).

the company founder's daughter.[215] In 2019, the Commerce Department put additional restrictions on Huawei for violating U.S. sanctions against Iran that prohibited American companies from doing business with the company without a special federal license.[216] In 2020, the United States would expand its restrictions and sanctions on Huawei by banning the use of American software or equipment in computer chips designed by the company and sold to the company.[217] Because of the prevalent use of American software and equipment in chip production around the world, this latest sanction further crippled Huawei's ability to do business.[218] As a coda, Ms. Meng was released in 2021 after a controversial exchange of seized business executives, which resulted from years of tense negotiations among Canada, China, and the United States.[219]

In terms of TikTok, in 2020, then President Trump ordered TikTok's China-based parent company, ByteDance, to sell its controlling stake in the company or be forced to shut down its operations in the United States.[220] TikTok is a popular video-sharing social media platform where users of the app can create and share videos with other users.[221] In 2020, TikTok reportedly had "100 million monthly active U.S. users."[222] This popularity raised U.S. national security concerns that the company would gather huge droves of private data from Americans and share it with the Chinese government for espionage, surveillance, and other nefarious ends.[223] In response to the executive action by the Trump Administration, ByteDance entered into advanced discussions to

---

[215] Tracy Sherlock & Dan Bilefsky, *Extradition of Huawei Executive Clears Major Legal Hurdle in Canada*, N.Y. TIMES, May 28, 2020, at A19.

[216] Lohr, *supra* note 9; Addition of Entities to the Entity List, 84 Fed. Reg. 22,963 (May 21, 2019) (codified at 15 C.F.R. pt. 744) (issuing a new, final rule adding Huawei to the Entity List, and putting restrictions on business dealings with Huawei).

[217] McCabe & Zhong, *supra* note 208.

[218] *Id.*

[219] Chris Buckley & Katie Benner, *Arrested Executive Returned to China in Exchange for Seized Canadians*, N.Y. TIMES, Sept. 26, 2021, at A6.

[220] Tali Arbel, *Trump Bans Dealings with Chinese Owners of TikTok, WeChat*, AP NEWS (Aug. 6, 2020), https://apnews.com/article/global-trade-ap-top-news-politics-asia-business-719d8c83f689929c9c9d8c9aa5593fc8 [https://perma.cc/K73J-X274].

[221] *See id.*; *Our Mission*, TIKTOK, https://www.tiktok.com/about?lang=en [https://perma.cc/L4LY-CXKQ].

[222] Alex Sherman, *TikTok Reveals Detailed User Numbers for the First Time*, CNBC, https://www.cnbc.com/2020/08/24/tiktok-reveals-us-global-user-growth-numbers-for-first-time.html [https://perma.cc/P4GS-CHQW] (Aug. 24, 2020, 6:33 PM).

[223] Claudia Biancotti, *The Growing Popularity of Chinese Social Media Outside China Poses New Risks in the West*, PETERSON INST. FOR INT'L ECON. (Jan. 11, 2019), https://www.piie.com/blogs/china-economic-watch/growing-popularity-chinese-social-media-outside-china-poses-new-risks [https://perma.cc/3UJV-GYPR].

sell parts of TikTok to American companies Oracle and Walmart.[224] Such a deal would be subject to the approval of the Chinese government, which was unlikely to assent to it.[225] In addition to pursuing partnerships with American companies in response to President Trump's executive order, ByteDance filed suit in federal court to overturn the ban.[226] In December 2020, a federal judge granted TikTok a victory by blocking President Trump's ban.[227] As a coda, in June 2021, newly elected President Biden revoked former President Trump's executive order on TikTok and replaced it with a broader, more precise executive order focused on protecting the data of Americans from foreign adversaries, namely foreign technology companies.[228]

The episodes involving Huawei and TikTok are not isolated incidents between China and the United States; instead, they are part of a larger business warfare battle in technology that reflects a generational struggle between these great powers.[229] The actions of the United States are neither unilateral nor unprovoked.[230] China has long placed restrictions, conditions, and bans on American companies, particularly technology companies, behind what some have dubbed "The Great Firewall of China."[231] As a result of Chinese government actions, many of the top American technology companies, like Google, Facebook, Snapchat, and Dropbox, are outright and officially banned in China.[232]

---

[224] *See* David McCabe, Ana Swanson & Michael J. de la Merced, *TikTok Deal in Question as Fine Print Is Disputed*, N.Y. TIMES, Sept. 22, 2020, at B1 (discussing the complicated deal regarding ownership of TikTok).

[225] *See id.*

[226] *See* Complaint for Injunctive and Declaratory Relief, TikTok Inc. v. Trump, 507 F. Supp. 3d 92 (D.D.C. 2020) (No. 20-cv-02658), *appeal dismissed sub nom.*, TikTok Inc. v. Biden, No. 20-cv-02658, 2021 WL 3082803 (D.C. Cir. July 14, 2021); Bobby Allyn, *U.S. Judge Halts Trump's TikTok Ban, the 2nd Court to Fully Block the Action*, NPR (Dec. 7, 2020), https://www.npr.org/2020/12/07/944039053/u-s-judge-halts-trumps-tiktok-ban-the-2nd-court-to-fully-block-the-action [https://perma.cc/YSW9-FBAC].

[227] *TikTok Inc.*, 507 F. Supp. 3d at 73 (granting TikTok's preliminary injunction).

[228] *See* Exec. Order No. 14034, 86 Fed. Reg. 31,423 (June 11, 2021); Katie Rogers & Cecilia Kang, *Biden Order Overrides TikTok Ban*, N.Y. TIMES, June 10, 2021, at B1.

[229] *See* KAI-FU LEE, AI SUPERPOWERS: CHINA, SILICON VALLEY, AND THE NEW WORLD ORDER 228–32 (2018); Rui Zhong, Opinion, *It's Getting Harder for Tech Companies to Bridge the US-China Divide*, MIT TECH. REV. (Sept. 21, 2020), https://www.technologyreview.com/2020/09/21/1008627/us-china-tiktok-wechat-ban-tech-policy-opinion/ [https://perma.cc/YHJ6-2QPV].

[230] *See* James Andrew Lewis, *Tech Crisis with China*, CTR. FOR STRATEGIC INT'L STUD. (Aug. 7, 2020), https://www.csis.org/analysis/tech-crisis-china [https://perma.cc/935A-83GM] (describing the history and landscape surrounding the United States' actions regarding China and technology).

[231] *See* Geremie R. Barme & Sang Ye, *The Great Firewall of China*, WIRED (June 1, 1997), https://www.wired.com/1997/06/china-3/ [https://perma.cc/BFY2-G3SZ] (documenting China's historical state control of the Internet and technology).

[232] Paige Leskin, *Here Are All the Major US Tech Companies Blocked Behind China's 'Great Firewall,'* INSIDER, https://www.businessinsider.com/major-us-tech-companies-blocked-from-operating-in-china-2019-5 [https://perma.cc/54C8-93C4] (Oct. 10, 2019).

China's "Great Firewall" is coupled with what some experts have dubbed a "Great Cannon" that has operationalized years of cyberattacks and aggressions on American private businesses and government agencies to steal intellectual property, disrupt operations, or commit espionage.[233] These actions were done to advance the intertwined interests of the Chinese government and Chinese businesses.[234] Thus, it is not entirely surprising that the United States has responded more aggressively in the last few years. At the end of 2020, the United States prohibited Americans from investing in companies that it believed had ties to the Chinese military, including some of the largest technology companies based in China and listed on American stock exchanges.[235] Accordingly, in early 2021, the New York Stock Exchange moved to delist several multi-billion dollar Chinese companies in response to the order.[236] Additionally, later in 2021, the Securities and Exchange Commission warned about investing in Chinese companies and moved to increase scrutiny of companies attempting to raise capital listed in the United States.[237]

As the United States and China continue to compete for global supremacy and influence in the coming years and decades, American and Chinese businesses will continue to find themselves in the crossfires of the business warfare between these two powerful nations.[238]

* * *

The business warfare episodes highlighted here involving the United States, Russia, Iran, and China are not isolated incidents, but rather reflective of larger trends in international affairs and conflicts. Rather than engage in costly, uncertain, and bloody traditional battles, adversaries are antagonizing one another through their business and economic interests. To be sure, business

---

[233] *See, e.g.*, Bill Marczak et al., *China's Great Cannon*, THE CITIZEN LAB (Apr. 10, 2015), https://citizenlab.ca/2015/04/chinas-great-cannon/ [https://perma.cc/Q28H-NDMB] (describing China's "Great Cannon"); Katie Benner & Nicole Perlroth, *Hackers Backed by China Had Broad Scope, U.S. Says*, N.Y. TIMES, Sept. 17, 2020, at A21 (discussing China-backed hackers' cyberattacks).

[234] BROSE, *supra* note 15, at 140.

[235] Ana Swanson, *Trump Bars Investment in Chinese Companies with Links to Military*, N.Y. TIMES, Nov. 13, 2020, at B5.

[236] Press Release, Intercont'l Exch., NYSE Announces Suspension Date for Securities of Three Issuers and Proceeds with Delisting (Jan. 6, 2021), https://ir.theice.com/press/news-details/2021/NYSE-Announces-Suspension-Date-for-Securities-of-Three-Issuers-and-Proceeds-with-Delisting/default.aspx [https://perma.cc/5CBE-DXDT]; Alan Rappeport, *In Second Reversal, Exchange Will Delist 3 Chinese Companies*, N.Y. TIMES, Jan. 7, 2021, at B4.

[237] *See* Gary Gensler, *Statement on Investor Protection Related to Recent Developments in China*, U.S. SEC. & EXCH. COMM'N (July 30, 2021), https://www.sec.gov/news/public-statement/gensler-2021-07-30 [https://perma.cc/AG8H-HNS3].

[238] *See* BROSE, *supra* note 15, at 87–95; RAPHAEL S. COHEN ET AL., RAND CORP., THE FUTURE OF WARFARE IN 2030, at 30 (2020), https://www.rand.org/content/dam/rand/pubs/research_reports/RR2800/RR2849z1/RAND_RR2849z1.pdf [https://perma.cc/7GDX-MG7H] (predicting that financial and economic power trends will dictate how future wars are fought).

warfare is not entirely new, but its intensity, volume, and variation has shifted and will likely increase over time.

III. Critical Legal and Practical Tensions

The unpredictability and savagery of new wars and conflicts often render laws and norms of past and peace inadequate.[239] Conceptions and visions of war and peace have evolved over time, with the differences between war and peace becoming less and less distinct.[240] Many of the old rules, paradigms, and ways of the past are not suitable for addressing some of the challenges of the present and the emerging future of war and peace.[241] Cicero, the great Roman politician and philosopher, stated, "In time of war, law is silent."[242] This is the fundamental legal and practical quandary of business warfare. There are few clear examples of roadmaps or battle plans from the past to address this new type of threat that inextricably intertwines national security, economic order, and private firms.[243] The challenge posed by the rising specter of business warfare finds root in deep legal and practical tensions between the longstanding international laws of war and the shifting realities of modern business. In particular, Section A of this Part first discusses the rising economic impact resulting from business warfare.[244] Second, Section B explains the tension that business hostilities create because of the lack of clear international law.[245] Third, Section C considers the various views on cyberattacks, and whether they constitute actual acts of war.[246] Fourth and lastly, Section D examines the problematic and complicated nature of cyberattacks conducted by non-state actors.[247]

---

[239] *See* Lin, *supra* note 14, at 1412–26 (discussing the increasing importance of concerns such as financial aggression, cyberattacks, and the role of non-state actors, in the evolving business warfare landscape).

[240] *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.").

[241] *See* Lin, *supra* note 14, at 1412 & n.200 (citing Koh, *supra* note 15, at 1772 ("Increasingly, we find ourselves addressing twenty-first-century challenges with twentieth-century laws.")).

[242] *See id.* & n.198 (quoting Mary L. Dudziak, War Time: An Idea, Its History, Its Consequences 3 (2012) (quoting Cicero)).

[243] *See* Heath, *supra* note 7, at 1096 ("The collision between national security and the economic order is a troubling and difficult problem.").

[244] *See infra* notes 248–264 and accompanying text.

[245] *See infra* notes 265–280 and accompanying text.

[246] *See infra* notes 281–304 and accompanying text.

[247] *See infra* notes 305–320 and accompanying text.

A. Of Economic Impact

One of the chief tensions of business warfare is its unintended domestic and global economic impact as countries engage in inextricably braided national security and economic strategies.[248] Attacking another country's businesses could not only hurt the target country, but also, the attacking countries, as other states retaliate with aggressions and sanctions of their own.[249] This ricocheting dynamic could leave some countries reticent to engage in business warfare or to retaliate after an act of business warfare despite having legitimate cause and political will to do so.[250] For instance, many companies and countries are reticent to antagonize or offend China because it represents one of the largest markets and manufacturing bases for many businesses.[251] This dynamic also motivates some countries to act aggressively to exploit the linkages in an interdependent global economic system.[252]

The modern world is deeply interdependent with allies as well as adversaries, especially on matters of economics.[253] An economic issue in one country—friend or foe—invariably creates ripple effects, some foreseeable, many unforeseeable.[254] This is true not just of economic distress in major economies like the United States and China, but also of smaller economies. For instance, the Greek debt crisis that started in 2009 had significant ripple effects across Europe, Asia, and the United States for nearly a decade because of the interlinked nature of global debt markets.[255]

Because business warfare often involves asymmetrical powers, some nations simply cannot engage in, or retaliate to business warfare in the same way as other nations because of competing economic and political considerations.

---

[248] *See* Heath, *supra* note 7, at 1024 ("The global economic order and the concept of national security are today deeply intertwined and difficult to disentangle.").

[249] HUFBAUER ET AL., *supra* note 106, at 108–13.

[250] *Id.* at 65–70.

[251] *See* F. Scott Kieff, *Business, Risk, & China's MCF: Modest Tools of Financial Regulation for a Time of Great Power Competition*, 88 GEO. WASH. L. REV. 1281, 1305 (2020) (opining that the "[t]he economic and social costs would be high" if tension between China and the United States escalated); Farhad Manjoo, Opinion, *Dealing with China Isn't Worth the Moral Cost*, N.Y. TIMES (Oct. 9, 2019), https://www.nytimes.com/2019/10/09/opinion/china-houston-rockets.html [https://perma.cc/9GGN-JMGQ] (arguing that China's authoritarian nature is not worth doing business with).

[252] WRIGHT, *supra* note 3, at 130.

[253] STIGLITZ, *supra* note 1, at 28–32.

[254] *See* Heath, *supra* note 7, at 1024 ("[I]n contrast to the Cold War period, major strategic rivals such as China, Russia, and the United States are also economic competitors within the same multilateral trading system.").

[255] *See* REBECCA M. NELSON, PAUL BELKIN & JAMES K. JACKSON, CONG. RSCH. SERV., R44155, THE GREEK DEBT CRISIS: OVERVIEW AND IMPLICATIONS FOR THE UNITED STATES 12–14 (2017) (describing the effects the Greek debt crisis had, and could have had, on the United States); MATTHEW LYNN, BUST: GREECE, THE EURO, AND THE SOVEREIGN DEBT CRISIS 260–62 (2011).

For instance, the United States, as an economic superpower with many high-value business targets, cannot engage in business warfare without serious consideration for its economic and political consequences.[256] American politicians thinking about the next election may not be able to fully engage in business warfare and risk a prolonged recession.[257] In contrast, authoritarian countries like Russia and China can engage in business warfare, including hurting their own domestic companies, with long term strategic imperatives in mind, without the same kind of fear of its political impact because they are not subject to free and fair democratic elections.[258]

That said, the United States in recent years has taken a more aggressive view on the links between national security and business interests, particularly when it involves foreign investments.[259] This is manifested partially in the more aggressive scrutiny of cross-border deals by the Committee on Foreign Investment in the United States (CFIUS), which has the power to block any transaction involving a foreign company or person.[260] CFIUS is an interagency committee headed by the Secretary of the Treasury that includes the Secretaries of State, Defense, Homeland Security, Commerce, and Energy, the Attorney General, and the U.S. Trade Representative.[261] The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) recently further enhanced and updated CFIUS's broad powers by expanding its scope, authority, and funding to review and block business transactions on national security grounds.[262] For instance, in 2019, the United States ordered a Chinese firm to

---

[256] HUFBAUER ET AL., *supra* note 106, at 90–95.

[257] *See, e.g.*, *id.* at 108–13 (discussing various political variables that accompany economic sanctions).

[258] *See, e.g.*, RUSH DOSHI, THE LONG GAME: CHINA'S GRAND STRATEGY TO DISPLACE AMERICAN ORDER 5–10 (2021) (describing China's authoritative regime, and its quest to become the world's number one power); TIMOTHY FRYE, WEAK STRONGMAN: THE LIMITS OF POWER IN PUTIN'S RUSSIA 66–72 (2021) (discussing Russia's lack of open and free elections); Austin Carr & Coco Liu, *Beijing's Tech Crackdown*, BLOOMBERG BUSINESSWEEK, Aug. 2, 2021, at 17, 17–18 (reporting on Chinese government action against domestic technology companies as means to gain greater control over private businesses); Matt Pottinger, Essay, *Beijing's American Hustle: How Chinese Grand Strategy Exploits U.S. Power*, FOREIGN AFFS., Sept./Oct. 2021, at 102, 102.

[259] *See* Tarbert, *supra* note 15, at 1492–1503 (documenting the rise in CFIUS investigations when foreign investment is involved).

[260] *See* 31 C.F.R. § 800.101 (2021); Amy Deen Westbrook, *Securing the Nation or Entrenching the Board? The Evolution of CFIUS Review of Corporate Acquisitions*, 102 MARQ. L. REV. 643, 647–55 (2019) (stating that the President can block a transaction by or with a foreign individual if it threatens to impair national security).

[261] *CFIUS Overview*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-overview [https://perma.cc/SY3Q-JNAK].

[262] *See Summary of the Foreign Investment Risk Review Modernization Act of 2018*, U.S. DEP'T OF THE TREASURY, https://www.treasury.gov/resource-center/international/Documents/Summary-of-FIRRMA.pdf [https://perma.cc/N9Q5-KKV5] (summarizing the updates and enhanced scope of

sell its holdings in Grindr, "the largest social-networking app for gay, bi, trans, and queer people" for fear of the Chinese government using the personal data on the app for blackmail.[263] Again, in 2020, CFIUS blocked a Chinese company from purchasing a fertility clinic in San Diego near strategic military bases for fear that the Chinese government would acquire and exploit sensitive health and genetic information of American military personnel.[264]

Nevertheless, despite a more aggressive posture by the United States in recent years, the economic impact of business warfare remains a key consideration in this new mode of battle.

B. Of Business Hostilities

One of the fundamental tensions in business warfare is the fact that there are no clear, longstanding laws or widely accepted norms governing attacks that are economic and financial in nature, even though the damage can be quite devastating in many respects.[265] The international laws and norms of war—the *jus ad bellum* and *jus in bello* principles—have long understood and defined war and wartime conduct primarily in the context of armed conflicts between and among nations.[266] These laws and norms did not fully contemplate a world where nations would target individual businesses of their adversaries, and individual businesses would become as valuable and important as entire nation-

---

CFIUS); Stephanie Zable, *The Foreign Investment Risk Review Modernization Act of 2018*, LAWFARE (Aug. 2, 2018), https://www.lawfareblog.com/foreign-investment-risk-review-modernization-act-2018 [https://perma.cc/UX5G-KRG7] (describing the updates to CFIUS and national security that FIRRMA will provide).

[263] Georgia Wells & Kate O'Keeffe, *U.S. Orders Chinese Firm to Sell Dating App Grindr Over Blackmail Risk*, WALL ST. J., https://www.wsj.com/articles/u-s-orders-chinese-company-to-sell-grindr-app-11553717942 [https://perma.cc/3WF9-YJ2M] (Mar. 27, 2019); *see About*, GRINDR, https://www.grindr.com/about/ [https://perma.cc/2DER-5GZT] (describing Grindr as an app for members of the LGBTQ+ community).

[264] Eamon Javers, *U.S. Blocked Chinese Purchase of San Diego Fertility Clinic Over Medical Data Security Concerns*, CNBC, https://www.cnbc.com/2020/10/16/trump-administration-blocked-chinese-purchase-of-us-fertility-clinic.html [https://perma.cc/3LWR-Q2TF] (Oct. 16, 2020, 9:00 AM).

[265] *See* Lin, *supra* note 14, at 1413 & n.203 (first citing MELZER, *supra* note 18, at 71–73 (describing the concept of a civilian in international armed conflict); then citing Waxman, *supra* note 18, at 422 (explaining that the wide-ranging, unconventional nature of cyberattacks precludes them from existing bans against traditional military attacks and "is part of what makes international legal interpretation or regulation in this area so difficult")).

[266] *See id.* at 1412 & n.201 (first citing Todd C. Huntley & Andrew D. Levitz, *Controlling the Use of Power in the Shadows: Challenges in the Application of* Jus in Bello *to Clandestine and Unconventional Warfare Activities*, 5 HARV. NAT'L SEC. J. 461, 461–63 (2014) (explaining how nonstate terrorist organizations challenge conventional war and peace legal standards); then citing Waxman, *supra* note 18, at 424–25 (discussing the historical rules governing war with the modern cyberattacks)).

states. The laws and norms did not fully comprehend a world where everything would become part of warfare and national security.[267]

Traditionally, international laws and norms governing war reflected the view that economic hostilities are best understood through frameworks of commerce, crime, and diplomacy, but not warfare.[268] The laws of war have long understood that economic coercion is generally not considered a prohibited use of force for purposes of international law.[269] When nations were working on the United Nations Charter in the aftermath of World War II, they openly considered and rejected the view that economic coercion should be a prohibited use of force among warring nations.[270] In fact, since its formation, the United Nations and its individual member states have regularly used economic sanctions as a key enforcement mechanism, thereby establishing the international norm that economically coercive or harmful policy actions are not illegal or prohibited uses of force among and between nations in conflict.[271]

Although international investment and trade law offer some avenues for redress against acts of economic hostility, such as through bodies like the World Trade Organization (WTO), these are often too slow and ill-suited to address urgent acts of aggressions against select businesses, particularly aggressions that are part of a concerted effort to attack a country.[272] International investment and trade laws are not well designed to address economic hostilities that impact both domestic economic issues and national security issues that

---

[267] *See* ROSA BROOKS, HOW EVERYTHING BECAME WAR AND THE MILITARY BECAME EVERYTHING 12–14 (2016) (describing the transition to the current state of modern "war" and the broad role that U.S. soldiers currently play).

[268] *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 15, at 840 (discussing challenges of 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). For further discussion about the applicability of international norms of war, *infra* 269–271, to business transactions, see Lin, *supra* note 14, at 1412–13.

[269] *See* Lin, *supra* note 14, at 1413 & n.205 (citing 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.")).

[270] *See id.* & n.206 (citing U.N. Conference on International Organization, *Addition to Chapter XII Submitted by the Brazilian Delegation*, U.N. Doc. 2, G/7 (e)(4), at 252–53 (May 6, 1945)).

[271] *See id.* & n.208 (citing Gervais, *supra* note 269, at 551 ("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.")).

[272] *See, e.g.*, KRISTEN HOPEWELL, BREAKING THE WTO: HOW EMERGING POWERS DISRUPTED THE NEOLIBERAL PROJECT 3–10 (2016) (discussing the limitations of the WTO in an era of emerging nations unwilling to subject themselves to its rules); Farah Stockman, Opinion, *The W.T.O.'s Midlife Crisis*, N.Y. TIMES, Dec. 18, 2020, at A18 (noting the problems of the WTO).

implicate foreign affairs.[273] These laws were never intended to govern hostilities in the new era of business warfare, where longstanding borderlines concerning economic and non-economic aggressions have broken down.

Furthermore, the historical demarcation between economic and non-economic hostilities has become less meaningful and more complicated with modern business warfare.[274] Direct hostile actions against an individual business with the intent to harm another sovereign state blurs the economic and non-economic triggers for the laws of war. This is particularly true because acts of business warfare often do not distinguish between civilians and non-civilians.[275]

Actions against American businesses in the last decade alone highlight some of the fading away of old understandings of war, or a greater willingness by some international principals to push the bounds of longstanding norms.[276] China has been suspected of concerted state-sponsored cyberattacks and espionage against private American businesses for many years, aimed at stealing critical intellectual property for its own businesses and national defense.[277] The Russians have hacked into the NASDAQ and many other private and government financial institutions with the intent to plunder and destabilize capital

---

[273] *See, e.g.*, Timothy Meyer & Ganesh Sitaraman, *Trade and the Separation of Powers*, 107 CALIF. L. REV. 583, 585–87 (2019) (discussing the competing, dominant domestic economic policy and foreign affairs paradigms of viewing trade laws).

[274] *See* Tom J. Farer, Editorial Comment, *Political and Economic Coercion in Contemporary International Law*, 79 AM. J. INT'L L. 405, 408–09 (1985) (highlighting how certain economic sanctions push the boundaries of international law); John Richardson, *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*, 29 J. MARSHALL J. COMPUT. & INFO. L. 1, 11 (2011) ("Damage to these institutions . . . while not destroying physical infrastructure, can have a far greater impact on a state's economy and its social infrastructure."); Heath, *supra* note 7, at 1024 ("Today, national security has evolved to address a range of threats, including non-state actors and nonmilitary and nonhuman threats, such as economic crises . . . .").

[275] *See* Jensen, *supra* note 15, at 1534–35 (discussing how "civilian-owned-and-operated networks and systems" are not controlled or protected by the U.S. government, but are used as the primary source of government communications, including classified communications); Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1524 (2013) (noting the problem that much of the world's infrastructure is dual use, serving a state's civilians and a state's government and military).

[276] *See* Waxman, *supra* note 18, at 436 (arguing for wartime hostilities to include aggressions like "a take-down of banking systems, causing cascades of financial panic").

[277] *See, e.g.*, Ariana Eunjung Cha & Ellen Nakashima, *Google Attack Part of Vast Campaign*, WASH. POST, Jan. 14, 2010, at A1 (detailing China's cyberattacks on private U.S. companies); Dune Lawrence & Michael Riley, *A Portrait of a Chinese Hacker*, BLOOMBERG BUSINESSWEEK, Feb. 18, 2013, at 54, 56 (same); David E. Sanger, David Barboza & Nicole Perlroth, *China's Army Seen as Tied to Hacking Against U.S.*, N.Y. TIMES, Feb. 19, 2013, at A1 (describing China's military as initiating cyberattacks); David E. Sanger & Mark Landler, *U.S. and China Will Hold Talks About Hacking*, N.Y. TIMES, June 2, 2013, at A1 (documenting a growing threat of cyberattacks).

markets.[278] Iran has worked to destabilize our banking system through persistent cyberattacks on our largest financial companies, like Bank of America, Citigroup, and JPMorgan Chase.[279] Had any of these countries used soldiers to physically trespass on the premises of an American government agency or contractor with the intent to destroy it, there would be little debate under traditional understandings of the laws and norms of war as to whether it violated such standards. Because American private businesses, rather than government actors, face these aggressions, which are often by way of cyber tools, the legal repercussions are less clear, even though the impact is clearly devastating.

This fundamental tension between the traditional understandings of law and the contemporary realities of war and conflict among nations will persist as business warfare grows more prevalent. As cool and cold wars grow warmer and hotter, the antiquated demarcations between economic and non-economic, private and public, and peace and war will fade away and give rise to more vexing tensions concerning business hostilities.[280]

C. Of Cyberattacks

The laws and norms of war established decades ago in the post-World War II period dominated by foot soldiers, bombs, and bullets are not well-suited to govern the cyberweapons and cyberattacks common in today's business warfare.[281] Cyberweapons are appealing because they are "so cheap to develop and so easy to hide" relative to traditional arms.[282] Legal and practical tensions arise relating to business warfare because there is no clear, broad consensus among critical international stakeholders on fundamental issues con-

[278] *See* Michael Riley, *How Russian Hackers Stole the Nasdaq*, BLOOMBERG BUSINESSWEEK, July 21, 2014, at 40, 42; Benjamin Weiser, *3 Men Are Charged with Serving as Secret Agents for Russia in New York*, N.Y. TIMES, Jan. 27, 2015, at A16.

[279] *See* Lin, *supra* note 14, at 1414–15; *see, e.g.*, Perlroth & Hardy, *supra* note 140 (documenting the effects of serious cyberattacks on American banks).

[280] *See generally* NOAH FELDMAN, COOL WAR: THE FUTURE OF GLOBAL COMPETITION (2013) (studying the brewing conflict and competition between China and the United States); Hal Brands & John Lewis Gaddis, *The New Cold War: America, China, and the Echoes of History*, FOREIGN AFFS. (Nov./Dec. 2021), https://www.foreignaffairs.com/articles/united-states/2021-10-19/new-cold-war [https://perma.cc/Z3XG-Y6MC] (discussing a new and different conflict dynamic between the United States and China).

[281] *See* SANGER, *supra* note 15, at 295–300; Shin-yi Peng, *Cybersecurity Threats and the WTO National Security Exceptions*, 18 J. INT'L ECON. L. 449, 450–55 (2015) (questioning how the WTO would resolve cyberattacks).

[282] *See* SANGER, *supra* note 15, at xii ("Cyberweapons are so cheap to develop and so easy to hide that they have proven irresistible.").

cerning cyberattacks.[283] Chief among them are interrelated issues of governance, jurisdiction, and methods and effects.

First, there are disputes among key international stakeholders on the most appropriate approach for governing cyber issues, which has created a void in international law on cyberattacks.[284] Although traditional warfare and armed conflict are largely governed by over a century of established and widely agreed upon rules and norms, business warfare involving cyberweapons lacks such widely agreed-upon rules among key nations.[285] The United States generally prefers a model of cyber governance rooted in existing rules, customs, and norms of international law, whereby states, international organizations, and private actors all share a role in governance.[286] Alternatively, China and Russia generally favor a nation-oriented model of governance that gives individual sovereign states most of the regulatory power over cyberspace.[287] Not surprisingly, each of these global powers has acted in accordance with their preferred view of governance. The United States has pushed for more collaborations and wider acceptance on cyber issues based on existing international law principles and practices.[288] China and Russia, on the other hand, have promulgated a series of laws that empower them with greater control over cyber issues within their respective countries.[289] For example, in early 2015, pursuant to preference of cyberspace governance, China issued a series of regulations mandating

---

[283] *See* 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, 180–82 (2006) (arguing for a separate convention for cyberattacks); Hathaway et al., *supra* note 15, at 840 ("[A]pplying the existing law of war framework to cyber-attacks is extraordinarily challenging."); Hollis, *supra* note 148, 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: LAW AND ETHICS FOR VIRTUAL CONFLICTS 3, 6–15 (Jens David Ohlin, Kevin Govern & Claire Finkelstein eds., 2015) (expounding on the differences between traditional wars and cyberwars).

[284] *See* Martha Finnemore & Duncan B. Hollis, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, 31 EUR. J. INT'L L. 969, 970–74 (2020) (finding that cyberattack victims fail to invoke international law).

[285] *See* Lin, *supra* note 14, at 1419 & n.241 (citing KENNEDY, *supra* note 240, at 46–63).

[286] *See id.* & n.242 (citing Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 321 (2015) (noting the differences in approach between the United States and China and Russia)); EXEC. OFF. OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 22 (2011) (stating American commitment to "[p]romote and enhance multi-stakeholder venues for the discussion of Internet governance issues" (emphasis omitted)).

[287] *See* Lin, *supra* note 14, at 1420 & n.244 (citing Eichensehr, *supra* note 286, at 320–21).

[288] *See infra* note 304 and accompanying text (describing the American approach to cyber warfare).

[289] *See infra* note 290 (describing China's new laws restricting cyber activities); *supra* note 132 (describing Russia's laws regarding cyber tracking).

foreign and domestic companies with operations in China to give the government "backdoor" access to all of their technological systems in the country.[290]

Second, cyberattacks used with business warfare create tensions concerning legal and practical issues of jurisdiction.[291] Under international law, a nation-state can generally govern people and activities within its borders, but cyberattacks in business warfare give little to no respect for national borders.[292] Traditional wars and armed conflicts occur within less disputed jurisdictions, be it "land, air, sea, [or] space," and are defined by laws and norms rooted in geographic boundaries.[293] Cyberattacks in business warfare occur in cyberspace, but require real world actions and impose real effects on multiple sovereigns, therefore rendering geographically-bound tools of enforcement less potent. For instance, an Iranian cyberattack against American investment bank Goldman Sachs' operations around the world could originate in Moscow using servers based across countries in Europe and Asia and affect operations throughout multiple continents. Presuming that attribution is even possible, how should the United States respond to such an aggression across so many jurisdictions on behalf of a private company?[294] To date, there remains no global consensus or strategy to answer this type of question.[295] That said, it is

---

[290] *See* Andrew Jacobs, *China Further Tightens Grip on the Internet*, N.Y. TIMES, Jan. 30, 2015, at A1 (discussing China's implementation of strict regulations concerning the Internet); Paul Mozur & Jane Perlez, *China Halts New Policy on Tech for Banks*, N.Y. TIMES, Apr. 17, 2015, at B1 (detailing China's suspension of a policy that would have effectively barred foreign technology companies from China's banking sector).

[291] *See* Lin, *supra* note 14, at 1416 & n.220 (first citing David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996) ("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."); then citing Lawrence Lessig, Commentary, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 514–22 (1999) (describing various regulatory challenges posed by the amorphous boundaries of cyberspace); and then citing May, *supra* note 283, at 6).

[292] *See id.* & n.221 (first citing 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."); then citing ROBERT K. KNAKE, COUNCIL ON FOREIGN RELS., INTERNET GOVERNANCE IN AN AGE OF CYBER INSECURITY 16 (2010) ("Whereas national legal authority is bounded by borders, the Internet is not."); and then citing Kristen E. Eichensehr, *Cyberwar & International Law Step Zero*, 50 TEX. INT'L L.J. 357, 368 (2015) ("[I]nternational law has traditionally operated at the level of sovereign States . . . .")).

[293] *See* Hathaway et al., *supra* note 15, 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.").

[294] *See* Finnemore & Hollis, *supra* note 284, at 974–77 (discussing the attribution challenges related to cyberattacks).

[295] *See* Eichensehr, *supra* note 15, at 523 ("[A]ttributing cyberattacks to individual perpetrators and especially to states that direct the attacks remains complicated because it involves unsettled legal and political issues."); Waxman, *supra* note 18, at 444 (discussing the difficulties of attribution).

hard to imagine that the United States would go to war with another country because of a destructive cyberattack on Goldman Sachs, Facebook, or another prominent American company. Although many countries, including the United States, China, and Iran, have openly recognized cyberspace as a military domain for purposes of international conflict, there remains no shared understanding on the critical questions of jurisdiction.[296]

Third, the methods and effects of cyberattacks used with business warfare present vexing practical and legal tensions when juxtaposed with traditional legal norms and rules governing war and armed conflict.[297] In terms of methods, cyberweapons are usually not designed to harm adversaries in the same violent or fatal manner as traditional weapons of war, like foot soldiers, bombs, and bullets.[298] Traditional definitions of wartime concepts like illegal use of force and armed conflict seem inappropriate for cyberweapons and cyberattacks that can manifest in so many different forms.[299] Furthermore, in terms of effects, business warfare cyberattacks are often designed to destabilize and damage an adversary's economy, rather than produce human casualties or a regime change. This can manifest in a wide variety of consequences that span from the temporary denial of critical company services to the destruction of a nuclear weapons facility.[300] Given the plethora of methods and effects, it can be incredibly difficult to apply international rules and norms designed for ag-

---

[296] *See* OFF. OF THE SEC'Y OF DEF., ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA 2013, at 37 (2013); Eichensehr, *supra* note 286, at 329–30.

[297] *See, e.g.*, Eichensehr, *supra* note 292, at 375–79 (discussing the need for laws of war to better address cyberattacks).

[298] *See* Lin, *supra* note 14, at 1417 & n.229 (first citing Hathaway et al., *supra* note 15, at 845 (discussing competing legal views on cyberattacks); then citing Duncan B. Hollis, *Re-thinking the Boundaries of Law in Cyberspace: A Duty to Hack?*, *in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS, *supra* note 283, at 129, 140 (highlighting difficulties of applying traditional legal doctrines to cyberattacks)).

[299] *See, e.g.*, Sean Watts, *Low-Intensity Cyber Operations and the Principle of Non-intervention*, *in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS, *supra* note 283, at 249, 249–51 (discussing non-intervention in response to low-intensity cyber operations); David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SEC. L. & POL'Y 87, 90–100 (2010) (discussing whether cyberattacks can constitute an armed attack); Hollis, *supra* note 148, at 1027–28 (describing nebulous classifications for aggressions in cyberspace); 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, 208–10 (2002) (questioning whether an attack on a nation's computer network constitutes an illegal use of force under traditional international law).

[300] *See* Broad et al., *supra* note 152 (describing the Israeli attack on Iranian nuclear operations); Hathaway et al., *supra* note 15, at 836 (asserting that "[c]yber-warfare can also constitute both cyber-attack and cyber-crime"); Perlroth, *supra* note 139 (describing the Iranian cyberattack which shut-down major U.S. banks).

gressions that kill humans and physically destroy government structures, to attacks that disrupt and decimate business computer systems.[301]

Although many of the aforementioned fundamental legal issues concerning cyberattacks remain unresolved among key players in the international community, it is important to note that significant progress has been made to promote some norms in cyberspace in recent years.[302] Efforts like the NATO-initiated *Tallinn Manual on the International Law Applicable to Cyber Warfare*, the *Wassenaar Arrangement*, an agreement governing international arms sales that included intrusion software as a restricted dual-use technology, and the *United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace* are all meaningful steps forward.[303] Additionally, the United States and other nations have taken initiative to better protect their respective homelands in the face of growing cyber threats, even while a larger global consensus remains elusive.[304] Nevertheless, much more progress is needed on the vexing legal and normative issues surrounding cyberattacks as business warfare grows more pernicious and prevalent.

D. Of Non-state Actors

Non-state actors—such as stateless terrorist organizations—can present thorny legal and practical challenges for nations and the international community, because many of the established rules and norms governing war and

---

[301] *See* Lin, *supra* note 14, at 1419 & n.238 (first citing Hathaway et al., *supra* note 15, at 826; then citing Hollis, *supra* note 148, at 1045 (opining on the challenges of translating existing rules of conflict into the context of cyberattacks); then citing William J. Lynn III, Essay, *Defending a New Domain: The Pentagon's Cyberstrategy*, FOREIGN AFFS., Sept./Oct. 2010, at 97, 108 ("The cyberthreat does not involve the existential implications ushered in by the nuclear age . . . ."); and then citing Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, International Law in Cyberspace, Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *in* 54 HARV. INT'L L.J. ONLINE 1, 3 (2012), https://harvardilj.org/wp-content/uploads/sites/15/2012/12/Koh-Speech-to-Publish1.pdf [https://perma.cc/5FEZ-DWQ2] (noting that "international law principles do apply in cyberspace," but they create a large number of difficult legal issues (emphasis omitted))).

[302] Hathaway et al., *supra* note 15, at 859–77 (providing an overview of a patchwork of international law relating to cyberattacks).

[303] *See* Lin, *supra* note 14, at 1420–21, 1421 & nn.250–51. *See generally* INT'L GRP. OF EXPERTS AT THE INVITATION OF THE NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013); THE WASSENAAR ARRANGEMENT, http://www.wassenaar.org [https://perma.cc/VJS9-M8D8]; *Group of Government Experts*, UNITED NATIONS, https://www.un.org/disarmament/group-of-governmental-experts/ [https://perma.cc/LR7J-7YJS].

[304] *See, e.g.*, Gary Corn, *SolarWinds Is Bad, but Retreat from Defend Forward Would Be Worse*, LAWFARE (Jan. 14, 2021), https://www.lawfareblog.com/solarwinds-bad-retreat-defend-forward-would-be-worse [https://perma.cc/PUZ4-4AY9] (discussing two new cybersecurity operational approaches initiated by the United States in 2018).

armed conflicts are designed with nation-states in mind.[305] This is particularly true as non-state actors engage in business warfare using cyberweapons, making these challenges more pressing.[306] The tensions concerning non-state actors involved in business warfare are based on the limitations that exist by the very nature of them lacking a sovereign state.

Because non-state actors lack a traditional state and all the features that come with it, like an internationally recognized government and national assets, nation-states are limited in how they can deal with them. For one, nation-states can readily enter into legal agreements that govern their wartime behavior and reasonably expect one another to cooperatively abide by them.[307] The same kind of accord and reciprocity, however, cannot be as easily achieved with stateless terrorist organizations.[308] Any agreements between and among states would not be binding on non-state actors.[309] Furthermore, it is much harder to hold a non-state actor accountable for aggressions in business warfare relative to

---

[305] *See* Kenneth Anderson, Professor of L., Wash. Coll. of L. Am. U., U.S. Counterterrorism Policy and Superpower Compliance with International Human Rights Norms, Speech Delivered to the *Fordham International Law Journal*'s Guantanamo Invitational Colloquium (Nov. 29, 2006), *in* 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.").

[306] *See, e.g.*, Gabriella Blum & Philip 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 about non-state actors); Katyal & Tribe, *supra* note 15, at 1259–60 (highlighting the constitutional challenges involved with trying terrorists); Michael N. Schmitt, Bellum Americanum: *The U.S. View of Twenty-First Century War and Its Possible Implications 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 . . . .").

[307] *See* Lin, *supra* note 14, at 1423 & n.261 (first citing ANDREW T. GUZMAN, HOW INTERNATIONAL LAW WORKS: A RATIONAL CHOICE THEORY 18 (2008) (describing how and why nations cooperate); then citing 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); and then citing 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.")).

[308] *See, e.g.*, Richemond-Barak, *supra* note 307, at 328 ("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.").

[309] *See, e.g.*, Eichensehr, *supra* note 286, 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.").

nation-states.[310] With state-based adversaries, traditional tools of international law and diplomacy can be used to hold them accountable (to some extent) for breaches of wartime laws and norms.[311] For instance, in recent years, the United States has taken actions against Russia and China in response and retaliation for cyberattacks on American public and private interests.[312] Non-state adversaries like hacker collectives, terrorists, and lone-wolf combatants are frequently much more difficult to trace and find, let alone hold accountable, because they do not have obvious targets for response and retaliation.[313]

A further complication concerning non-state actors is the fact that these adversaries frequently hide and reside in locales governed by less-than-friendly or cooperative states, creating practical obstacles to pursue non-state actors within these foreign nations.[314] The United States confronted this issue in the pursuit of Osama Bin Laden and Al-Qaeda in the years after the September 11, 2001 attacks.[315] The pursuit ultimately resulted in a raid on a compound in Pa-

---

[310] *See, e.g.*, Gabriella Blum, *On a Differential Law of War*, 52 HARV. INT'L L.J. 163, 168–73 (2011) (discussing the equal application of international law among states)).

[311] *See* Lin, *supra* note 14, at 1424 & n.268 (first citing DAVID A. BALDWIN, ECONOMIC STATECRAFT 130–33 (new ed. 2020) (explaining state accountability mechanisms via economic sanctions and relationships); then citing Eichensehr, *supra* note 286, at 370–71 (noting the difficulty in holding non-state actors accountable with traditional international laws and norms); and then 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)).

[312] *See* David E. Sanger, *U.S. Decides to Retaliate Against China's Hacking*, N.Y. TIMES, Aug. 1, 2015, at A6 (noting President Barack Obama's determination that the United States must retaliate against China for its theft of personal information of more than 20 million Americans); Nicole Perlroth, *U.S. Issues Sanctions on Russian Center Involved in Potentially Deadly Cyberattacks*, N.Y. TIMES (Oct. 23, 2020), https://www.nytimes.com/2020/10/23/us/politics/russia-cyberattack-saudi-plant-sanctions.html [https://perma.cc/4Z75-BP4R] (describing the economic sanctions enacted by the United States against a Russian government research organization because of the cyberattack the organization conducted against a Saudi petrochemical company).

[313] *See* Lin, *supra* note 14, at 1424 & n.269 (first citing 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 noncompliance."); and then citing Joseph S. Nye Jr., *Nuclear Lessons for Cyber Security?*, STRATEGIC STUD. Q., Winter 2011, at 18, 20 (examining how state actors might be more vulnerable to cyberattacks by non-state actors)).

[314] *See* 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, 38 (2009) (acknowledging the rigidity of the *jus ad bellum* framework as applied to non-state actor cyberattacks, while noting some avenues for recourse and retaliation available to victim-states); George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079, 1190–95 (2000) (discussing the issue of neutral states in cyberwarfare).

[315] PETER L. BERGEN, MANHUNT: THE TEN-YEAR SEARCH FOR BIN LADEN FROM 9/11 TO ABBOTTABAD 20–30 (2012).

kistan to kill Bin Laden without informing Pakistan, and a costly two-decade war in Afghanistan.[316]

Although many legal and practical issues concerning non-state actors have achieved greater understanding in the decades since the September 11, 2001 attacks on the United States, much more progress needs to be made in developing a set of workable tools, weapons, and strategies as non-state actors engage in business warfare to disrupt the affairs of nation-states.[317]

* * *

War—its sources, methods, and effects—moves and changes swiftly, but the laws often evolve so slowly.[318] Business warfare is yet another iteration of modern conflict. The core of the Geneva Conventions, the monumental corpus of treaties established after World War II governing wartime conduct, remains largely unchanged, despite many changes in warfare and weaponry over the years.[319] This disconnect between the laws and realities of war leads to legal and practical tensions as nations try to solve difficult problems of business warfare.[320] As they attempt to safeguard their interests in an uncertain, dangerous world, they especially must confront the tensions that business warfare poses for economic impact, business hostilities, cyberattacks, and non-state actors.

IV. KEY RECOMMENDATIONS

The emergence of business warfare will require new international laws and norms concerning war and armed conflict to better address the new tensions and questions it presents for the global order.[321] While those larger issues are being debated and deliberated through lengthy legal and political processes, nation-states and businesses—particularly the United States and American

---

[316] *See id.* at 196–201; Thomas Gibbons-Neff, *A Solemn Pullout in a Lost Fight's Last Hours*, N.Y. TIMES, Aug. 31, 2021, at A1.

[317] *See* David Ronfeldt & John Arquilla, *What Next for Networks and Netwars?*, *in* NETWORKS AND NETWARS: THE FUTURE OF TERROR, CRIME, AND MILITANCY 311, 350–54 (John Arquilla & David Ronfeldt eds., 2001) (discussing the need to develop a variety of mechanism to address the non-state actors).

[318] *See* Eichensehr, *supra* note 292, 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."); INTEL. & NAT'L SEC. ALL., CYBER INTELLIGENCE: SETTING THE LANDSCAPE FOR AN EMERGING DISCIPLINE 6 (2011) ("National and international laws, regulations, and enforcement are still struggling to catch up to cyber activities worldwide."); Koh, *supra* note 15, at 1772 (remarking on the legal challenges posed by emerging technologies).

[319] Hathaway et al., *supra* note 15, at 840.

[320] *See, e.g.*, Eichensehr, *supra* note 286, at 380 ("The intersovereign issues posed by cyber are more complicated and will probably take even longer to solve.").

[321] *See* Heath, *supra* note 7, at 1096–98 (calling for development of a new international legal model to deal with the emergence of new age cyber warfare).

businesses—can take immediate actions to better safeguard their interests against the threats of business warfare. In particular, Section A of this Part first suggests that nations and companies can lead initiatives on business war games.[322] Next, Section B advocates for an increase in cybersecurity incentives.[323] Lastly, Section C proposes that diversification of supply chains and markets is needed in order to better prepare for the perils of business warfare.[324]

A. Business War Games

Nation-states and businesses should regularly engage in war games between and among themselves to better prepare for the threats of business warfare.[325] War games have long been used by nations to improve their readiness and defenses.[326] One of the earliest forms of war games was a variation of present-day chess that dates back to 3000 B.C.[327] War games simulate potential attacks and decision points in a semi-controlled environment where its participants can test and assess their strengths and vulnerabilities in a dynamic setting.[328] During and since the Cold War, the Pentagon has regularly run hypothetical and operational exercises to test the efficacy of the U.S. military in facing adverse scenarios around the world.[329] Just as war games have long as-

[322] *See infra* notes 325–346 and accompanying text.

[323] *See infra* notes 347–368 and accompanying text.

[324] *See infra* notes 369–384 and accompanying text.

[325] *See, e.g.*, Baradaran, *supra* note 15, at 1319 (suggesting financial war games for businesses as beneficial); John Crawford, *Wargaming Financial Crises: The Problem of (In)experience and Regulator Expertise*, 34 REV. BANKING & FIN. L. 111, 168–74 (2014) (discussing the benefits of using financial crises simulations).

[326] *See* Lin, *supra* note 14, at 1437 & n.335 (citing Baradaran, *supra* note 15, 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."); Elizabeth M. Bartels, Building Better Games for National Security Policy Analysis: Towards a Social Scientific Approach 61–63 (Mar. 2020) (Ph.D. dissertation, Pardee RAND Graduate School), https://www.rand.org/content/dam/rand/pubs/rgs_dissertations/RGSD400/RGSD437/RAND_RGSD437.pdf [https://perma.cc/HSG8-2KMB] (discussing the design of war games to best prepare a party)).

[327] *See* Lin, *supra* note 14, at 1437 & n.336 (citing FRANCIS J. MCHUGH, FUNDAMENTALS OF WAR GAMING 27 (3d ed. 1966)).

[328] *See id.* & n.337 (citing JOINT CHIEFS OF STAFF, JOINT PUB. 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 395 (Nov. 8, 2010, as amended through Dec. 31, 2010), https://www.hsdl.org/?abstract&did=11391 [https://perma.cc/J2RC-NHUR] (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")).

[329] *See id.* & n.338 (citing Thomas B. Allen, *Twilight Zone in the Pentagon*, *in* THE COLD WAR: A MILITARY HISTORY 230, 230–34 (Robert Cowley ed., 2005) (describing how war games operated)); ANTHONY H. CORDESMAN & ASHLEY HESS, THE EVOLVING MILITARY BALANCE IN THE KOREAN PENINSULA AND NORTHEAST ASIA, VOLUME II: CONVENTIONAL BALANCE, ASYMMETRIC FORCES, AND US FORCES 178 (2013) (recounting war games between the United States and South Korea designed by the Pentagon); Ralf Emmers, *Security and Power Balancing: Singapore's Response to the US Rebalance in Asia*, *in* THE NEW US STRATEGY TOWARDS ASIA: ADAPTING TO THE

sisted policy-makers in preparing for war in the theaters of land, air, and sea, these recommended war games can help public and private institutions better steel themselves for conflicts in the theater of business.[330]

These war games should be done by and between governments and businesses, because modern business warfare frequently involves both public and private actors. The federal government can run business war games to better prepare American interests for business warfare.[331] Various Departments and agencies of the federal government, like Defense, Homeland Security, and the Treasury, can lead and coordinate these exercises, marshalling military, public, and private expertise and resources. The participation of private business is particularly important in these exercises because businesses are often on the frontline of modern conflicts.[332]

Similarly, large private businesses should stress test their defenses and capabilities by regularly running war games within their institutions. These internal war games would push corporate boards and senior executives to carry out their fiduciary duties to their shareholders more thoughtfully, as they think collectively and strategically about their risks, and move beyond siloed, tactical processes that have become all too common in contemporary business management.[333] While businesses alone usually cannot and should not defend

---

AMERICAN PIVOT 143, 147 (William T. Tow & Douglas Stuart eds., 2015) (documenting the war games performed with Singapore).

[330] For an introduction to the role of war games throughout history, see generally MCHUGH, *supra* note 327; PETER P. PERLA, THE ART OF WARGAMING: A GUIDE FOR PROFESSIONALS AND HOBBYISTS (1990); JON PETERSON, PLAYING AT THE WORLD: A HISTORY OF SIMULATING WARS, PEOPLE AND FANTASTIC ADVENTURES, FROM CHESS TO ROLE-PLAYING GAMES (2012); MICHAEL VICKERS & ROBERT MARTINAGE, CTR. FOR STRATEGIC & BUDGETARY ASSESSMENTS, FUTURE WARFARE 20XX WARGAME SERIES: LESSONS LEARNED REPORT (2001), https://indianstrategicknowledgeonline.com/web/R.20011201.FutureWarXX.pdf [https://perma.cc/GCW8-AGH2].

[331] *See, e.g.*, Robert C. Rubel, *The Epistemology of War Gaming*, 59 NAVAL WAR COLL. 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.").

[332] *See* Lin, *supra* note 14, at 1436 & n.331 (first citing Richard K. Gordon, *Losing the War Against Dirty Money: Rethinking Global Standards on Preventing Money Laundering and Terrorism Financing*, 21 DUKE J. COMPAR. & INT'L L. 503, 510–17 (2011) (explicating on the important role of private firms in combatting terrorism financing); then citing Sales, *supra* note 275, at 1567 ("[T]he private sector should play an active role in establishing industry-wide cyber-security standards . . . ."); then citing Matthew Goldstein, *Wall St. and Law Firm Plan Cooperative Body to Bolster Online Security*, N.Y. TIMES, Feb. 24, 2015, at B7 (describing the current threats of large cyberattacks bringing together private companies, such as banks and law firms, and the federal government; and then citing DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 8–9 (2011), https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf [https://perma.cc/A784-BVAA] (urging more frequent collaborations between government entities and private businesses to bolster cybersecurity)).

[333] *See* GILLIAN TETT, THE SILO EFFECT: THE PERIL OF EXPERTISE AND THE PROMISE OF BREAKING DOWN BARRIERS, at ix–xii (2015) (observing how during the 2008 financial crisis,

themselves against attacks by a foreign nation-state, these internal war games could help boards and senior executives understand their institutional vulnerabilities and better prepare for potential risks, responses, and recoveries when an attack eventually occurs on their businesses.[334] War games can help situate executives to think from a more militaristic perspective and to work through a military-like "kill chain," a combat decision process that prevents unnecessary casualties and damage within the context of their enterprises.[335] These war games can also help public and private institutions play out and imagine formerly unseen attacks and approaches in warfare that leverage new technology and business practices, like cryptocurrencies and artificial intelligence.[336] Although some businesses may prefer to remain neutral or above the fray on conflicts between states, recent history, particularly in the cyber realm, suggests that neutrality is not an option for many businesses.[337]

This recommendation for business war games that includes governments and businesses is not radical or entirely unprecedented. 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 economic weapons against the United States by a foreign nation like China.[338] 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.[339] And for more than a decade following the financial crisis of 2008, the Federal Reserve has been

---

"[p]eople were trapped inside their little specialist departments, social groups, teams, or pockets of knowledge . . . inside their silos").

[334] STANLEY MCCHRYSTAL & ANNA BUTRICO, RISK: A USER'S GUIDE 270–72 (2021).

[335] BROSE, *supra* note 15, at xviii–xix.

[336] *See* ANNIE JACOBSEN, THE PENTAGON'S BRAIN: AN UNCENSORED HISTORY OF DARPA, AMERICA'S TOP-SECRET MILITARY RESEARCH AGENCY 313–30 (2015) (chronicling how war games aided government officials in responding to unexpected attacks and extreme events); Bailey Reutzel, *What Is Cryptocurrency? Here's What You Need to Know About Blockchain, Coins and More*, CNBC (Sept. 22, 2021), https://www.cnbc.com/select/what-is-cryptocurrency/ [https://perma.cc/9JA3-359W] (explaining cryptocurrency); Darrell M. West, *What Is Artificial Intelligence?*, BROOKINGS (Oct. 4, 2018), https://www.brookings.edu/research/what-is-artificial-intelligence/ [https://perma.cc/ZRG7-AR7G] (explaining artificial intelligence).

[337] *See* Eichensehr, *supra* note 78, at 696–73 (discussing the limitations of neutrality as relating to businesses in conflicts among nation-states).

[338] *See* Lin, *supra* note 14, at 1439 & n.347 (citing ERIC J. WEINER, THE SHADOW MARKET: HOW A GROUP OF WEALTHY NATIONS AND POWERFUL INVESTORS SECRETLY DOMINATE THE WORLD 13–14 (2010)).

[339] *See id.* & n.349 (first citing SIFMA, FACT SHEET: QUANTUM DAWN 3, at 1, https://www.sifma.org/wp-content/uploads/2017/09/quantum-dawn-fact-sheet.pdf [https://perma.cc/5DQ9-G6GB]; then citing SIFMA, STANDING TOGETHER FOR FINANCIAL INDUSTRY CYBER RESILIENCE: QUANTUM DAWN 3 AFTER-ACTION REPORT 3 (2015), https://www.sifma.org/wp-content/uploads/2017/04/QuantumDawn-3-After-Action-Report.pdf [https://perma.cc/T7J9-WAZ7]).

running regular stress tests on systemically important financial institutions.[340] That said, governments and businesses across various industries can become more thoughtfully engaged in business war gaming to better think like the enemy and gain valuable insights as the threats of business warfare loom larger with each passing day.[341]

Although no war game can perfectly simulate or recreate an actual battle or attack, a good war game can nonetheless be incredibly illuminating to public and private institutions, pushing them to prepare for business warfare so that they do not react in a haphazard, untested manner during times of crisis.[342] Well-designed war games can create cross-learning opportunities for businesses and governments to anticipate and prepare for the threats of contemporary business warfare.[343] Better preparation, although not always highly predictive, is especially necessary given the high velocity and uncertainty of global economic and financial markets.[344] As former President Dwight Eisenhower, who served as the Supreme Commander of the Allied Expeditionary Force in Europe in World War II, famously remarked about war planning: "In preparing for battle I have always found that plans are useless, but planning is indispensable."[345] Therefore, as the threats of business warfare grow, better planning for it through smart war games that thoughtfully engage nation-states and private firms is urgently indispensable.[346]

B. Cybersecurity Guidance and Incentives

Governments, particularly the U.S. federal government, should regularly provide strong cybersecurity guidance and incentives for private firms across

---

[340] *See* RIEL & MARTIN, *supra* note 15 (discussing the importance of integrative thinking in business strategy and management).

[341] *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 112, at 34–35 (discussing the need to gather better information to combat 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).

[342] *See* Lin, *supra* note 14, at 1439 & n.350 (citing 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 policy-makers following the 2008 financial crisis)).

[343] *See* Eduardo Jany, *Operational Resilience: Lessons Learned from Military History*, CAPCO INST. J. FIN. TRANSFORMATION, May 2021, at 140, 140 (stating that testing and war games can help prepare an entity for warfare); Wheeler, *supra* note 17, 135 (recounting that military history is full of "debris of armies" that did not anticipate threats).

[344] *See, e.g.*, Tom C.W. Lin, *The New Investor*, 60 UCLA L. REV. 678, 711–13 (2013) (discussing the high speed of modern financial markets).

[345] Lin, *supra* note 14, at 1439 & n.351 (citing RICHARD M. NIXON, SIX CRISES 235 (1962) (quoting Dwight Eisenhower)).

[346] *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).

all industries, given that so much of business warfare involves attacks and aggressions on private actors in cyberspace. Thoughtful government leadership and coordination is necessary to counteract some of the collective action problems and easy business inclinations to underinvest in cybersecurity upgrades.[347] A smart and strong public-private partnership is necessary to confront the cybersecurity challenges of business warfare.[348]

First, in terms of guidance, the federal government should work with leading companies in the private sector to provide guidance on the latest and best cybersecurity protocols and practices. Although some industries, like the financial, utilities, and technology sectors, have significant regulatory guidance and compliance resources on cybersecurity, others do not.[349] For instance, in the financial sector, regulators like the Federal Reserve and the Securities and Exchange Commission regularly offer cybersecurity-related guidance for financial institutions.[350] As such, large financial institutions are often at the forefront of significant regular investments in cybersecurity to protect their companies.[351]

Nevertheless, it is not enough that only some companies in some industries have strong cybersecurity. Because of the interlinked nature of modern information networks and an interdependent global economic system, all of the public and private sectors must be vigilant and work jointly in their cybersecurity defenses, as one vulnerability can lead to destructive cascades and grave systemic risk across multiple industries and countries.[352] The serious Russian

---

[347] *See* Bambauer, *supra* note 15, at 1031 (noting that "cybersecurity suffers from a collective-action problem," resulting in businesses resorting to individual institutional interests that may run contrary to the greater interest).

[348] *See* Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 470–71 (2017) (discussing the emergence of the public-private partnership).

[349] *See, e.g.*, Tom C.W. Lin, *Compliance, Technology, and Modern Finance*, 11 BROOK. J. CORP. FIN. & COM. L. 159, 175–77 (2016) (discussing the significant cybersecurity and compliance resources expended annually by some large financial firm).

[350] *See generally* OFF. OF COMPLIANCE INSPECTIONS & EXAMINATIONS, U.S. SEC. & EXCH. COMM'N, CYBERSECURITY AND RESILIENCY OBSERVATIONS, https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf [https://perma.cc/53UX-GN5U]; FED. FIN. INSTS. EXAMINATION COUNCIL, CYBERSECURITY ASSESSMENT TOOL (2017), https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf [https://perma.cc/V2FY-2RGJ].

[351] JPMorgan Chase & Co., Annual Report (Form 10-K), at 142 (Feb. 24, 2015) (spending $250 million toward cybersecurity); 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.").

[352] *See, e.g.*, Lin, *supra* note 14, at 1392 (discussing attacks on financial institutions that trigger "vicious cycles of volatility for the entire financial infrastructure as actions cascade and generate feedback loops and spillover effects of serious systemic, adverse consequences"); Amir E. Khandani, Andrew W. Lo & Robert C. Merton, *Systemic Risk and the Refinancing Ratchet Effect* 48 (Harv. Bus. Sch., Working Paper No. 10-023, 2010), https://www.hbs.edu/ris/Publication%20Files/10-023_035a0d8f-7670-4e6e-bf56-f452282277d8.pdf [https://perma.cc/V5B7-Z7X4] ("[S]ystemic risk . . . arises

cyberattack of 2020 was the result of a vulnerability in the widely used software of the publicly-traded company, SolarWinds, and the breach of the public and private institutions was discovered in part by FireEye, another publicly-traded company.[353] As such, to better fortify cybersecurity in the presence of business warfare, governments and businesses must work together in crafting and following best practices guidance.

Second, in addition to guidance, the federal government should provide meaningful incentives to encourage private firms to regularly upgrade their cybersecurity systems.[354] Because much of the technological infrastructure that makes up the cyber domain is owned and operated by private firms that are frequently motivated by profits, smart incentives may be necessary to encourage timely cybersecurity improvements, investments, and information-sharing.[355] In the absence of public incentives, investments in cybersecurity may remain stagnant as businesses focus on short-term cost savings and profits, rather than long-term stability and systemic safety.[356] Furthermore, properly designed incentives can encourage more proactive and timely investments and information-sharing, rather than reactionary moves in response to a major security breach from the private sector.[357]

Informed guidance, coupled with smart incentives, can manifest in a number of policies to enhance corporate cybersecurity for public and private

---

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.").

[353] David E. Sanger, *Russians Hack U.S. Agencies in Bold Attack*, N.Y. TIMES, Dec. 14, 2020, at A1.

[354] *See* Sales, *supra* note 275, at 1538–39 (discussing the incentive to protect consumer data in the Gramm-Leach-Bliley Act); Daniel Huang, Emily Glazer & Danny Yadron, *Financial Firms Boost Cybersecurity Funds*, WALL. ST. J., Nov. 17, 2014, at C3 (noting the plans of financial firms to boost cybersecurity spending).

[355] *See* Eichensehr, *supra* note 286, at 350–51 ("[P]rivate parties own the majority of the underlying infrastructure that supports the cyber domain.").

[356] *See* STEWART BAKER, SHAUN WATERMAN & GEORGE IVANOV, MCAFEE, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 14 (2009) (noting that cost was a frequently cited obstacle to ensuring adequate security for an entity's networks); JOEL BRENNER, AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE 239 (2011) (discussing the vulnerabilities to private businesses from a failure to invest in and install available technology); N.Y. DEP'T OF FIN. SERVS., REPORT ON CYBER SECURITY IN THE BANKING SECTOR 11 (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).

[357] *See, e.g.*, NISSEN ET AL., *supra* note 17, at 35 (advocating for tax incentives to help private entities invest in cybersecurity); Jessica Silver-Greenberg & Matthew Goldstein, *After Breach, Push to Close Security Gaps*, N.Y. TIMES, Oct. 22, 2014, at B1 (discussing the push by government officials to bolster cybersecurity after a large cyberattack on JPMorgan Chase); Derek E. Bambauer, *Schrödinger's Cybersecurity*, 48 U.C. DAVIS L. REV. 791, 848–50 (2015) (discussing various political tools for encouraging better cybersecurity); Tom C.W. Lin, *The New Financial Industry*, 65 ALA. L. REV. 567, 614 (2014) ("[A]s a matter of principle, policymakers should use affirmative incentives in addition to negative penalties to help encourage industry participants to behave sensibly.").

sectors alike. Tax policy, for example, can be used to encourage companies to improve their cybersecurity readiness on a regular basis.[358] Through a mix of bonus depreciation, tax credits, and increased deductions, the government can encourage and subsidize the upgrades of outdated, vulnerable information systems and spur investment in more secure systems.[359] In the same way that the government used tax policy in the American Recovery and Reinvestment Act following the financial crisis of 2008 to incentivize private businesses to accelerate and enlarge capital investments to stimulate the economy, it can act similarly to enhance business cybersecurity.[360]

Additionally, the federal government can use its large procurement powers across all private sectors to encourage timely cybersecurity improvements by private firms, for example, by giving contracting preferences to firms that meet certain government cybersecurity benchmarks and conditions.[361] 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.[362] 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 cyber threats.[363] In fact, in 2015, the Office of Management and Budget initiated a review of current acquisition practices with an eye towards enhancing cybersecurity through

---

[358] *See* NISSEN ET AL., *supra* note 17, at 35 (suggesting that tax incentives are a viable option to spur businesses to invest in cybersecurity).

[359] *See* JANE G. GRAVELLE, CONG. RSCH. SERV., R43432, BONUS DEPRECIATION: ECONOMIC AND BUDGETARY ISSUES 4 (2014) (describing bonus depreciation); GARY GUENTHER, CONG. RSCH. SERV., RL31853, THE SECTION 179 AND SECTION 168(K) EXPENSING ALLOWANCES: CURRENT LAW AND ECONOMIC EFFECTS 1 (2018) (same); INTERNAL REVENUE SERV., HOW TO DEPRECIATE PROPERTY 3–14 (2021), https://www.irs.gov/pub/irs-pdf/p946.pdf [https://perma.cc/Y8WS-YE6R] (same); ERIC ZWICK & JAMES MAHON, DO FINANCIAL FRICTIONS AMPLIFY FISCAL POLICY? EVIDENCE FROM BUSINESS INVESTMENT STIMULUS 39 (2014), https://scholar.harvard.edu/files/zwick/files/stimulus.pdf [https://perma.cc/7W4Z-5W5D] (finding that policies, like tax incentives, that target investment decisions best propel firms to act); James M. Williamson & John L. Pender, *Economic Stimulus and the Tax Code: The Impact of the Gulf Opportunity Zone*, 44 PUB. FIN. REV. 415, 417–19 (2014) (discussing tax incentives post-Hurricane Katrina).

[360] *See* Lin, *supra* note 14, at 1429 & n.293 (citing *Business Provisions of the American Recovery and Reinvestment Act of 2009 (ARRA)*, INTERNAL REVENUE SERV. (May 2009), https://www.irs.gov/pub/irs-news/fs-09-11.pdf [https://perma.cc/E78Q-U78N]).

[361] *See id.* at 1430 & n.299 (first citing Bambauer, *supra* note 15, at 1062–64 (suggesting implementation of IT requirements as a condition of contracting with the government); then citing BAKER ET AL., *supra* note 356, at 14 (discussing underinvestment by private firms in cybersecurity)).

[362] *See id.* & n.300 (first citing Bambauer, *supra* note 15, at 1062–64 (noting the significant spending power of the U.S. government and how it can, and has, used this power to implement change in private entities); then citing Daniel P. Gitterman, *The American Presidency and the Power of the Purchaser*, 43 PRESIDENTIAL STUD. Q. 225, 225–29 (2013) (examining the power of the President to shape policy using procurement)).

[363] *See id.* & n.301 (citing 48 C.F.R. § 552.239-71 (2021) (mandating the contractor be responsible for IT security)).

the federal procurement process and has continued to seek ways to enhance cybersecurity in a similar fashion since then.[364]

Furthermore, carefully crafted legal safe harbors to shield companies from certain liabilities could encourage more timely information-sharing about cybersecurity vulnerabilities and threats with government agencies and other industry peers. In the absence of such protections, companies might be reticent to share critical information for fear of exposing themselves to lawsuits and other liabilities. In recent years, a few states and the federal government have proposed and adopted safe harbor provisions related to cyberattacks to encourage best practices on information-sharing and timely disclosures.[365] Nevertheless, these safe harbors thus far represent only small steps. More comprehensive efforts are needed to encourage businesses to adopt cybersecurity best practices and share breaches within their systems in a timely manner, in the best interests of the larger network.[366]

Although many large companies already invest significant resources in cybersecurity, many still do not.[367] To better protect against cyberattacks and other threats in cyberspace emanating from business warfare, all businesses and all industries could urgently use better guidance and incentives from the government. As former President Barack Obama remarked about cybersecurity in 2015: "[N]either government, nor the private sector can defend the nation alone. It's going to have to be a shared mission—government and industry

---

[364] *See id.* & n.302; *Our Focus Areas*, U.S. CHIEF INFO. OFFICERS COUNCIL, https://policy.cio.gov [https://perma.cc/J76Q-LW2N] (listing initiatives taken toward better cybersecurity).

[365] *See* David Farber, David Manek, Ted Theisen & Colleen Yushchak, *New Proposed Laws Include Safe Harbor When Aligned with NIST Privacy Framework*, JD SUPRA (Aug. 4, 2021), https://www.jdsupra.com/legalnews/new-proposed-laws-include-safe-harbor-2986211/ [https://perma.cc/ALS7-TL2P] (documenting the new trend in cybersecurity laws introducing safe harbor clauses); Cynthia Brumfield, *States Enact Safe Harbor Laws Against Cyberattacks, but Demand Adoption of Cybersecurity Frameworks*, CSO (Mar. 29, 2021), https://www.csoonline.com/article/3613176/states-enact-safe-harbor-laws-against-cyberattacks-but-demand-adoption-of-cybersecurity-frameworks.html [https://perma.cc/N9BC-PP3G] (discussing recent legislative initiatives to offer liability protection against cyberattacks, but only if the victim followed best security practices); Jeffrey T. Ganiban & Alex Eschenroeder, *HHS Issues Final Cybersecurity Safe Harbor and Exception*, NAT'L L. REV. (Dec. 15, 2020), https://www.natlawreview.com/article/hhs-issues-final-cybersecurity-safe-harbor-and-exception [https://perma.cc/WRC4-8VRQ] (discussing the safe harbor instituted under the Anti-Kickback Statute (the AKS Cybersecurity Safe Harbor)); Medicare and State Health Care Programs: Fraud and Abuse; Revisions to Safe Harbors Under the Anti-Kickback Statute, and Civil Monetary Penalty Rules Regarding Beneficiary Inducements, 85 Fed. Reg. 77,684 (Dec. 2, 2020) (to be codified at C.F.R. pt. 1001, 1003).

[366] NISSEN et al., *supra* note 17, at 30 (proposing litigation reform).

[367] Alex Blau, *The Behavioral Economics of Why Executives Underinvest in Cybersecurity*, HARV. BUS. REV. (June 7, 2017), https://hbr.org/2017/06/the-behavioral-economics-of-why-executives-underinvest-in-cybersecurity [https://perma.cc/5W24-QXTA] (discussing why entities underinvest in cybersecurity).

working hand in hand, as partners."[368] Importantly, as such, government efforts to develop cybersecurity guidance must reflect an iterative process that actively engages with industry leaders, capitalizing on their firsthand experience to inform policies and respond to emerging technologies.

C. Supply Chain and Market Diversification

Government and business leaders should work urgently and creatively to diversify their supply chains and markets to better steel themselves from the disruptions and threats of business warfare.[369] Toward that end, firms and nation-states should work together to create greater domestic capacity for certain key supplies, industries, and markets.

A more diversified supply chain and marketplace would allow businesses to better withstand aggressions from adversaries and engage in business warfare while mitigating economic blowback. For instance, a firm like Apple, which is largely reliant on contract manufacturers and rare earth suppliers in China, would be particularly vulnerable to punitive actions from the Chinese government.[370] Because Apple is one of the most valuable companies in the world and one of the most widely-held securities in the portfolios of Americans, a sustained attack on Apple could have serious repercussions on the American economy and psyche.

More troubling is that a single flawed or vulnerable supply chain component can create many soft points of entry for an adversary, especially when a foreign state serves as a critical node in the production process.[371] The unprecedented Russian hack of 2020 of American business and government interests was the result of a supply chain vulnerability, whereby adversaries used a third-party vendor's product to attack its target.[372] Similarly, the world currently relies heavily on two companies, Samsung and Taiwan Semiconductors

---

[368] Barack Obama, President, Remarks by the President at the National Cybersecurity Communications Integration Center (Jan. 13, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent [https://perma.cc/S7VN-SW9N].

[369] *See* Kevin B. Hendricks & Vinod R. Singhal, *Supply Chain Disruptions and Corporate Performance*, *in* SUPPLY CHAIN DISRUPTIONS: THEORY AND PRACTICE OF MANAGING RISK 1, 1–3 (Haresh Gurnani, Anuj Mehrotra & Saibal Ray eds., 2012) (discussing the recent immergence and focus on supply chains and their increased importance with globalization).

[370] *See* Tripp Mickle & Yoko Kubota, *Tim Cook and Apple Bet Everything on China. Then Coronavirus Hit.*, WALL ST. J., https://www.wsj.com/articles/tim-cook-and-apple-bet-everything-on-china-then-coronavirus-hit-11583172087 [https://perma.cc/L92Q-QEST] (Mar. 3, 2020).

[371] *See* CHINA STRATEGY GRP., ASYMMETRIC COMPETITION: A STRATEGY FOR CHINA & TECHNOLOGY 21–25 (2020), https://s3.documentcloud.org/documents/20463382/final-memo-china-strategy-group-axios-1.pdf [https://perma.cc/KE82-L7H8] (discussing the importance of decoupling critical technology supply chains between the United States and China for national security purposes).

[372] Sanger, *supra* note 353.

Manufacturing Company, for semiconductors that are essential for almost everything involving electronics, from automobiles to ventilators.[373] As such, a disruption of the production processes of either companies would have deleterious effects that would ripple across numerous countries and companies.[374]

Rather than becoming too reliant on one supply chain or one marketplace for inputs and revenues, firms should seek more diversification on these fronts, which would create greater resilience for them to weather attacks from adversaries in business warfare.[375] Admittedly, moves towards greater supply chain and market diversification could hurt short-term revenues and profits, which will likely make such moves difficult for myopic corporate executives.[376] Nevertheless, greater market and supply chain diversification should pay off over the long run for many businesses, providing greater stability to boards and shareholders.

In addition to firm-based efforts to diversify supply chains and markets, government agencies should work with key businesses to create domestic capacity for certain critical supplies and industries to blunt any deleterious economic impact that could result from business warfare.[377] Through a combination of mandates and incentives, governments can foster domestic capacity to support more diversified supply chains and markets.[378] This public-private effort would make nations better positioned to withstand attacks on their businesses and their economies in the same way that the United States possesses the National Strategic Stockpile for public health crises and the Strategic Petroleum Reserves for energy crises.[379] For instance, the federal government has

---

[373] EURASIA GRP., THE GEOPOLITICS OF SEMICONDUCTORS 3–5 (2020), https://www.eurasiagroup.net/files/upload/Geopolitics-Semiconductors.pdf [https://perma.cc/L8XP-FYKY].

[374] *Id.*

[375] There is a rich, longstanding management and economics literature on the benefits of market diversification for businesses. *See, e.g.*, Jean-Emile Denis & Daniel Depelteau, *Market Knowledge, Diversification and Export Expansion*, J. INT'L BUS. STUD., Fall 1985, at 77, 77–89 (discussing diversification); W. Chan Kim, Peter Hwang & Willem P. Burgers, *Multinationals' Diversification and the Risk-Return Trade-Off*, 14 STRATEGIC MGMT. J. 275, 275–86 (1993) (same); Cynthia A. Montgomery & Harbir Singh, *Diversification Strategy and Systemic Risk*, 5 STRATEGIC MGMT. J. 181, 182–88 (1984) (same); Sanjiv Talwar, *Preparing for Critical Disruption: A Perspective on Operational Resilience*, CAPCO INST. J. FIN. TRANSFORMATION, May 2021, at 14, 14–15 (same).

[376] *See* ROGER L. MARTIN, FIXING THE GAME: BUBBLES, CRASHES, AND WHAT CAPITALISM CAN LEARN FROM THE NFL 29 (2011) ("In the face of expectations that can run wild, CEOs have increasingly focused on what they can control: managing share price over the short run."); Tom C.W. Lin, *CEOs and Presidents*, 47 U.C. DAVIS L. REV. 1351, 1409–10 (2014) ("Too often, many modern CEOs are too myopic—too focused on next week and next quarter, rather than next year and the long-term horizon.").

[377] NISSEN et al., *supra* note 17, at 24–28.

[378] *Id.*

[379] *See Strategic National Stockpile*, OFF. OF THE ASSISTANT SEC'Y FOR PREPAREDNESS & RESPONSE, U.S. DEP'T OF HEALTH & HUM. SERVS. https://www.phe.gov/about/sns/Pages/default.aspx [https://perma.cc/K84Q-G2L6] (Aug. 9, 2021); *SPR Quick Facts*, OFF. OF FOSSIL ENERGY & CARBON

broad authority over private business under the Defense Production Act to mandate that firms create products for national security.[380]

During peace times when capital and supplies are free-flowing, creating domestic capacity for critical supplies and industries may seem unnecessary. During times of war and crises, however, the lack of domestic capacity for critical supplies and industries can render a nation particularly vulnerable. The COVID-19 pandemic made this uncomfortable truth evident in the United States. Thousands of Americans died each day as the county lacked the ready capacity to produce personal protective equipment, ventilators, swabs, and other critical supplies, the manufacturing of which is located primarily in China.[381] Rather than be subject to economic attack of foreign adversaries, governments should work proactively with the private sector to identify and create meaningful domestic capacity for certain critical supplies and industries. Not surprisingly, about one month into his presidency in 2021, President Biden ordered a review of the United States' critical supply chains "to ensure our economic prosperity and national security."[382]

To be clear, this recommendation should not be viewed as an opposition to the virtues of free and fair trade or the economic principles of comparative advantage that have produced incredible prosperity and wealth.[383] Rather, it should be understood as a sensible step that can better safeguard a country's interests in the face of rising threats of business warfare. Furthermore, even in the absence of ongoing or looming threats, greater market and supply chain

---

MGMT., https://www.energy.gov/fe/services/petroleum-reserves/strategic-petroleum-reserve [https://perma.cc/HFL9-XAUS].

[380] *See* Defense Production Act of 1950, 50 U.S.C. app. §§ 2061–2171; MICHAEL H. CECIRE & HEIDI M. PETERS, CONG. RSCH. SERV., R43767, THE DEFENSE PRODUCTION ACT OF 1950: HISTORY, AUTHORITIES, AND CONSIDERATIONS FOR CONGRESS 1 (2020).

[381] *See* Keith Bradsher, *Ahead of the Curve*, N.Y. TIMES, July 6, 2020, at B1 (noting China's dominance over pandemic supplies); Jennifer Cohen & Yana van der Meulen Rodgers, *Contributing Factors to Personal Protective Equipment Shortages During the COVID-19 Pandemic*, PREVENTIVE MED., Dec. 2020, Article 106263, at 1 (investigating the shortage in personal protective equipment during the COVID-19 pandemic, including major disruptions to the global supply chain).

[382] *Executive Order on America's Supply Chains*, WHITE HOUSE (Feb. 24, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/ [https://perma.cc/VE9M-H9HU].

[383] *See* THOMAS SOWELL, BASIC ECONOMICS: A COMMON SENSE GUIDE TO THE ECONOMY 479–82 (5th ed. 2015) (explaining the principle of comparative advantage as the basis for international free trade); PIERRE LEMIEUX, WHAT'S WRONG WITH PROTECTIONISM? ANSWERING COMMON OBJECTIONS TO FREE TRADE 8–16 (2018) (arguing that comparative advantage facilitates free trade that enhances the welfare of wealthy and poor nations); KIMBERLY CLAUSING, OPEN: THE PROGRESSIVE CASE FOR FREE TRADE, IMMIGRATION, AND GLOBAL CAPITAL 71 (2019) ("Both rich and poor countries benefit from trade, as economic growth and efficiency are enhanced. This does not mean, however, that every individual in a particular country will gain from trade. Many may find themselves working in far more competitive conditions.").

diversification will help better fortify our economic security and national security for an uncertain future.[384]

* * *

Business warfare will continue to impact many aspects of law, business, and society in ways large and small. While progress is being made on the longstanding geopolitical and international law issues affecting business warfare, the recommendations provided in this Article offer a workable trio of policies and actions that business and government leaders can take in the near-term to prepare for the inevitability of these attacks. Undoubtedly, the complex challenges of realizing these proposals will lie in the actual drafting, implementation, compliance, and enforcement of any new rules and policies. Nevertheless, the discussion here offers meaningful, principled guideposts for business and government leaders as they confront the challenges of modern business warfare.

CONCLUSION

The harsh and complicated realities of business warfare will present some of the most difficult decisions for political leaders, corporate executives, military commanders, legislators, and regulators for the foreseeable future. The convergence of global conflicts, private business, and war will have serious lingering legal, economic, and social implications. Contemporary business warfare threatens and impacts every nation, every firm, and every citizen.

This Article offers an original, critical perspective of this growing, contemporary war on business. It examines the combatants, targets, and weapons of this looming mode of conflict, highlights critical legal and practical tensions, and proposes workable initiatives to better protect business stakeholders and nations against the looming threats of business warfare. Throughout its examination, this Article is mindful of the serious military and national considerations implicated by this form of warfare, as well as the longstanding legal and political principles concerning economic hostilities that have made reforms in this area so elusive for companies and countries. Instead of advocating for an elegant, grand framework that may theoretically solve all of the challenges of business warfare or clearly redefine longstanding legal doctrines of war for a new age, this Article provides a more crosscutting, civilian-oriented perspective that advocates for three workable proposals. Although more modest in theory, they are more meaningful in practice. In particular, the Article argues for robust business war games, smart cybersecurity guidance

[384] *See, e.g.*, Madeleine Ngo & Ana Swanson, *Lack of Truckers Is Choking U.S. Supply Chain*, N.Y. TIMES, Nov. 10, 2021, at A1 (noting the problems associated with trucking shortages); Katie Rogers & Brad Plumer, *U.S. Moves to Fix Bottlenecks in Supply Chain*, N.Y. TIMES, June 9, 2021, at B3 (discussing actions taken to fix supply chain problems).

and incentives, as well as greater supply chain and market diversification as means to immediately confront the emerging threats and risks of business warfare while the larger issues of international and geopolitical consideration remain open. In the end, this Article hopes to provide a pragmatic framework for thinking, planning, and acting anew—with greater urgency—to address the dangers posed by business warfare.