ARTICLE

CYBER REALPOLITIK

JAMES DEVER[1] AND JACK DEVER[2]

[1] CPT James Dever is an active duty U.S. Army Judge Advocate. He is the Chief of Intelligence Law at the Intelligence Center of Excellence and HUMINT Training Joint Center of Excellence. He previously served at the Cyber Center of Excellence. Prior to the Army, CPT Dever worked at Deloitte Cyber Risk Services in Rosslyn, VA. At Deloitte, he partnered with the National Institute of Standards and Technology ("NIST") Trusted Identities in Cyberspace and Privacy Engineering programs. He also facilitated cyber security resilience protocols for the National Aeronautics and Space Administration (NASA). CPT Dever has published multiple law review articles and has spoken about cyber issues at the Congressional Cyber Security Caucus, NATO Allied Command, The U.S. Army Judge Advocate General's Legal Center & School, and New York University Law School. He is a member of The Journal of Law and Cyber Warfare editorial board. The views expressed by CPT Dever are his own and do not reflect the official policy or position of the U.S. Army, Department of Defense, or U.S. Government.

[2] John P. Dever Jr. is the Head of AML/Sanctions, Wholesale Financial Crimes Risk and Compliance at Wells Fargo. He was an Assistant U.S. Attorney for the Northern District of Illinois (Chicago), and prior to that, he was Assistant General Counsel in the Federal Bureau of Investigation's National Security Law Branch, Counterterrorism Division. He began his career as a U.S. Army Judge Advocate. He served multiple combat deployments to Iraq and Afghanistan and is the recipient of the Bronze Star and the Purple Heart Medals. He holds a LL.M. in National Security Law from The Georgetown University Law Center.

CONTENTS

I. INTRODUCTION

State-on-state conflict governed by generally clear rules of engagement was the predominant mode of warfare in the mid-twentieth century.[3] Now, almost two decades into the post-9/11 world, state and non-state actors, transnational terrorists, and cyber operators thrive in twilight zones of domestic and international law.[4] The past few years carry signs of troubles to come. Transnational terrorism, struck down in certain areas, but emboldened by twenty years of muddled U.S. and Allied counterterrorism policy, threatens again to break out of its Middle Eastern base.[5] China is stealing U.S. trade secrets at a rate beyond alarming and forcing American companies to work inside China or forfeit profitable trade deals.[6] Russia, a shadow of what it once was during the height of the Soviet Union,[7] now seeks to project strength through information warfare against the West.[8] North Korea too has learned how to fight in the cyber domain — its hackers rob banks worldwide and hold companies hostage through advanced cyber operations. [9] As sanctions continue to strangle Iran's economy, its cyber forces strike repeatedly at U.S. financial institutions in the hope of securing political and economic concessions.[10] To triumph in this complex and increasingly cyber-reliant world, the U.S. must accomplish four goals: (1) stop terrorist financing; (2) attribute and punish state and non-state malicious actors; (3) protect the private sector; and (4) realize a systematic, predictive method for cyber defense.

---

[3] Sean D. Murphy, *Evolving Geneva Convention Paradigms in the "War on Terrorism": Applying the Core Rules to the Release of Persons Deemed "Unprivileged Combatants,"* 75 GEO. WASH. L. REV. 1105, 1113 (2007).

[4] Rosa Ehrenreich Brooks, *War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror*, 153 U. PA. L. REV. 675, 677-80 (2004).

[5] Daniel L. Byman*, The Islamic State's Long-term Threat to the Middle East*, BROOKINGS (July 28, 2017), https://www.brookings.edu/blog/markaz/2017/07/28/the-islamic-states-long-term-threat-to-the-middle-east/ [https://perma.cc/73R8-UNL4].

[6] *See* Rogin, *infra* note 157.

[7] Ted Galen Carpenter, *Russia Is Not the Soviet Union*, CATO INST.: COMMENTARY (July 28, 2018), https://www.cato.org/publications/commentary/russia-not-soviet-union [https://perma.cc/KRQ7-TGAJ] ("The American public and U.S. policymakers both have an unfortunate tendency to conflate Russia with the Soviet Union. . . Russia's power is a pale shadow of the Soviet Union's.").

[8] *See* Heather Timmons, *Charted: Why Trump is Foolish to Treat Russia as an Equal Partner*, QUARTZ (July 18, 2018), https://qz.com/1331063/trump-putin-summit-why-russia-isnt-a-world-power-like-the-us-or-china/ [https://perma.cc/3NLT-3HP4] (discussing Russia's economic power versus other countries in the world, including China).

[9] Alex Hern, *North Korea is a Bigger Cyber-Attack Threat than Russia, Says Expert*, THE GUARDIAN (Feb. 26, 2018, 5:58 AM), https://www.theguardian.com/technology/2018/feb/26/north-korea-cyber-attack-threat-russia [https://perma.cc/3M7Y-BFRD].

[10] *See* discussion *infra* Section V.B.

II. NEW CONCEPTIONS OF WARFARE

A. Changing Norms

Rules in warfare date to ancient Greece.[11] Almost two thousand years later, during the rise of the early modern world a "series of treaties that formed the Peace of Westphalia [and] ended the Thirty Years War . . . created a system of legally equal [sovereignties]" and marked the beginning of international law as applied to state-on-state conflict.[12] A leap forward in what is now termed the Law of Armed Conflict[13] ("LOAC") occurred in 1863.[14] In the midst of the American Civil War, President Lincoln's Administration empowered Francis Lieber to write General Order No. 100, Instructions for the Government of Armies of the United States in the Field which provided "basic rules [regarding lawful and unlawful] combat, including [discussions] relating to the treatment of civilians" during hostilities.[15] General Order No. 100 became the template for all subsequent LOAC codes.[16] Most significantly, the 1949 Geneva Conventions, which are comprised of four treaties, were adopted after World War II to mandate humane treatment of persons in wartime.[17] The Geneva Conventions established rules that now appear straightforward when juxtaposed

[11] Rosa Ehrenreich Brooks, *War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror*, 153 U. PA. L. REV. 675, 688 (2004). *See, e.g.,* THE LANDMARK THUCYDIDES: A COMPREHENSIVE GUIDE TO THE PELOPONNESIAN WAR 192-93 (Robert B. Strassler ed. 1996) (discussing Athenian warfare and notions of what does not constitute treachery and perfidy on the battlefield).

[12] Sean Watts & Theodore Richard, *Baseline Territorial Sovereignty and Cyberspace*, 22 LEWIS & CLARK L. REV. 771, 795-96 (2018).

[13] Geoffrey S. Corn et al., *Belligerent Targeting and the Invalidity of a Least Harmful Means Rule*, 89 INT'L L. STUD. 536, 538 (2013).

[14] Brooks, *supra* note 11, at 688. *See also* U.S. DEP'T OF WAR, ADJUNCT GENERAL'S OFFICE, GEN. ORDER NO. 100, INSTRUCTIONS FOR THE GOVERNMENT OF THE ARMIES OF THE UNITED STATES IN THE FIELD (1863); Stephanie McCurry, *Enemy Women and the Laws of War in the American Civil War*, 35 L. & HIST. REV. 667 (2017) (detailing the hazards women faced in combat).

[15] Brooks, *supra* note 11, at 688.

[16] *See, e.g*., Geneva Convention Relative to the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Geneva Convention for the to the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Geneva Convention Relative to the Treatment of Prisoners of War art. 4(A)(2), Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Geneva Convention Relative To The Protection Of Civilian Persons In Time Of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287; Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, art. 1. Oct. 18, 1907). for an excellent overview of the Geneva Conventions see generally THE 1949 GENEVA CONVENTIONS: A COMMENTARY (Andrew Clapham et al. eds., 2015).

[17] *See generally* THE 1949 GENEVA CONVENTIONS: A COMMENTARY, *supra* note 16.

to the irregular twenty-first century conflicts pertaining to terrorists and non-state actors.[18] The Conventions established two main categories of persons or "statuses"—combatants and civilians.[19] Captured combatants were referred to as "prisoners of war" ("POWs") and this term was defined in the text.[20] The 1977 Additional Protocol I conveniently defined the term "civilians" in the negative such that everyone who is not a combatant is a civilian.[21]

The 9/11 attacks showed that traditional LOAC norms were inadequate to encompass the novel issues presented by the "War on Terror."[22] For instance, LOAC norms did not clarify whether the fight against Al Qaeda constituted an "armed conflict." Nor did it clarify the consequences, per the Geneva Conventions, of Taliban fighters failure to wear "uniforms or operate within a regular command structure"?[23] As Sean Murphy has argued:

> Many of the controversies [arose] because the two [operative] paradigms… within the Geneva Conventions – . . . 'international' armed conflict (i.e., conflict between two or more states[, or "IAC"]) and . . . 'noninternational' armed conflict between [intra-]state and nonstate actors ([usually deemed a civil war, or "NIAC"]) do not fit the [typology] of global terrorism, [which is the province of] transnational conflict [amongst] state and nonstate actors.[24]

Yet more difficult is the "unprivileged enemy belligerent" (UEB) category arising from NIACs and constituting persons, which encompasses one who:

> (A) has engaged in hostilities against the United States or its coalition partners; (B) has purposefully and materially supported hostilities against

---

[18] *See generally id*.

[19] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 51(3), *opened for signature* Dec. 12, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I].

[20] Geneva Convention Relative to the Treatment of Prisoners of War art. 4(A)(2), Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135.

[21] Protocol I, *supra* note 19. Protocol I explains the protections for victims of international armed conflicts. *Id.* Additional Protocol II provides protection for civilians in non-international armed conflicts. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, art. 13(3), *opened for signature* Dec. 12, 1977, 1125 U.N.T.S. 609 [hereinafter Protocol II].

[22] Sean D. Murphy, *Evolving Geneva Convention Paradigms in the "War on Terrorism": Applying the Core Rules to the Release of Persons Deemed "Unprivileged Combatants,"* 75 GEO. WASH. L. REV. 1105, 1105 (2007).

[23] *Id.* at 1106.

[24] *Id*. at 1113 ("The Geneva Conventions are [primarily] concerned with international armed conflicts between two [belligerent] states." It is of no moment if the states do or do not "formally recognize . . . the existence of a "war" [or if] they recognize [each other's legitimacy], [further,] the Conventions" are built upon the premise that uniformed combatants operating within regular armies constitute the opposing sides.).

> the United States or its coalition partners; or (C) was a part of al Qaeda at the time of the alleged offense under this chapter.[25]

As some have noted, "[t]his is a complex [but] vague definition."[26] In 1942, the U.S. Supreme Court in *Quirin* recognized the concept of "unlawful combatants" (*e.g.*, spies; enemy combatants not wearing uniforms behind enemy lines "for the purpose of waging war by destruction of life or property") as "familiar examples of belligerents who are generally deemed not to be entitled to the status of prisoners of war (POW), but to be offenders against the law of war."[27] From the U.S. perspective, "[a] UEB is . . . a combatant who is not entitled to the protections [afforded by] POW status because [they do] not meet the requirements" under Geneva Convention III."[28] Showcasing the extent to which the modern rules are a departure from the more clear-cut Geneva Conventions, a UEB in 2019 might be "[a] civilian directly participating in hostilities."[29] Further, most nations do not support the U.S. position and thus fail to recognize the UEB as a separate category distinct from lawful combatants and civilians.[30] In the complex post-9/11 world, the U.S. maintains UEBs can be lawfully detained until the end of hostilities.[31] Congress and the U.S. Supreme Court likewise endorse this position even though it continues to lack broad international support.[32]

The normative understandings regarding the application of *jus ad bellum*, the portion of international law governing when states may resort to force, changed tremendously since 9/11.[33] So too has *jus in bello*, the law regarding the conduct

---

[25] 10 U.S.C. § 948a(7) (2012).

[26] Russell Spivak, *"Born of Military Necessity:" Redesigning Military Commissions for the 21st Century*, 54 HARV. J. ON LEGIS. 301, 316 (2017).

[27] *Ex parte Quirin*, 317 U.S. 1, 31 (1942). For in-depth discussion regarding distinctions between unlawful combatants and unprivileged enemy belligerent*,* see RYAN DOWDY ET AL., THE JUDGE ADVOCATE GENERAL'S LEGAL CENTER AND SCHOOL LAW OF ARMED CONFLICT DESKBOOK 142 (Rachel S. Mangas et al., 16th ed. 2016), https://www.hqmc.marines.mil/Portals/135/JAO/2016%20LOAC%20Deskbook.pdf?ver=2018-08-07-124727-057 [https://perma.cc/ZK9J-USTQ].

[28] Geneva Convention III provides baseline protections for persons on the battlefield such as humane treatment and prohibits, *inter alia*, torture. Charles Pendleton Trumbull IV, *Analogies in Detentions: Distorting the Balance Between Military Necessity and Humanity*, 58 VA. J. INTL. L. 97, 107 (2018).

[29] Elisabeth Gilman, *The Case for Strategic U.S. Detention Policy*, 224 MIL. L. REV. 118, 157 (2016). Gilman, *supra* note 16.

[30] *Id.* at 158-60.

[31] Trumbull, *supra* note 28 at 114.

[32] *See* Nat'l Def. Authorization Act of 2012, 125 Stat. 1298 § 1021(b)(2) (2012); Hamdi v. Rumsfeld, 542 U.S. 507, 517, 521 (2004).

[33] Michael N. Schmitt, *Responding to Transnational Terrorism Under the Jus Ad Bellum: A Normative Framework*, 56 NAVAL L. REV. 1, 2 (2008).

of war.[34] While *jus ad bellum* is about finding peaceful ends to conflicts and balancing restraints on aggression with legitimate self-defense, *jus in bello* balances protection of humanitarian values or impulses with military necessity.[35] Pursuant to Article 2(4) of the United Nations ("UN") Charter, party states agree to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[36] There are two nearly unanimous exceptions to the general prohibition against the use of force.[37] Pursuant to Article 39, the first exception is when the Security Council determines that a breach of the peace, act of aggression, or threat to the peace exists and measures to resolve the situation through non-forceful means, as required by Article 41, have failed; the Council may then authorize the use of force to preserve or restore international peace and security pursuant to Article 42.[38] The second exception involves the customary international law norm of self-defense codified in Article 51 which states that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs."[39]

On September 12, 2001, the UN Security Council adopted Resolution 1386 whichrecognized the inherent right of individual or collective self-defense and thereby crystallized the acceptability of resorting to military force in response to transnational terrorism.[40] The Council "[u]nequivocally condemn[ed] in the strongest terms the horrifying terrorist attacks which took place on 11 September 2001 in New York, Washington, D.C. and Pennsylvania and regard[ed] such acts, like any act of international terrorism, as a threat to international peace and security."[41] Additionally, recognizing that terrorists obtaining money to recruit for, plan, and execute their missions is a condition precedent to most attacks, the Council in Resolution 1373 obliged states to cooperate against terrorist financing and freeze the financial assets of all persons who participate in, or facilitate, acts of terror.[42] Notwithstanding the Council's recognition of the grave

[34] *See* Matthew C. Waxman, *The Structure of Terrorism Threats and the Laws of War*, 20 DUKE J. COMP. & INT'L. L. 429, 447 (2010).

[35] *See* Gabriella Blum, *The Laws of War and the "Lesser Evil",* 35 YALE J. INT'L. L. 1, 7-9 (2010).

[36] U.N. Charter art. 2, ¶ 4.

[37] *Id.* arts. 39, 42, 51.

[38] *Id.* arts. 39, 42 ("Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations.").

[39] *Id.* art. 51.

[40] S.C. Res. 1368 (Sept. 12, 2001).

[41] *Id. See also* Schmitt, supra note 33, at 41.

[42] S.C. Res. 1373, ¶ 2 (Sept. 28, 2001).

threat terrorism poses to international peace and security, the right to act in self-defense against terrorism is not all-encompassing because defensive uses of force, to include force directed against non-state actors, must meet the nineteenth century "Caroline test" criteria of a "necessity of self-defense, instant, overwhelming, (and) leaving no moment for deliberation."[43]

B. Targeting Evolved

During the twentieth century, when the model of state-on-state conflict prevailed, the LOAC targeting analysis for standard rules of engagement was more straightforward because determinations often involved status-based as opposed to conduct-based targets.[44] Status-based targets are lawful combatants who, per Geneva Convention III requirements, act "[u]nder responsible command; [w]ear a fixed distinctive sign recognizable at a distance; [c]arry arms openly; and [a]bide by the laws of war."[45] In contrast, conduct-based targets consistently violate LOAC standards by, for example, attacking uniformed lawful combatants while wearing civilian clothes in order to blend and hide themselves within civilian populations.[46] Ahmad Fadhil Nazzal al-Khalaylah, who later renamed himself Abu Musab al-Zarqawi, was a notorious practitioner of perfidy and treachery in Iraq and routinely violated the rules of LOAC.[47] Al-Zarqawi and his followers were difficult to target in Iraq because they did not wear uniforms[48] and choose to commit on-camera beheadings in safe houses and bombing civilians over direct combat with U.S.-led coalition forces.[49] On June 8, 2006, a U.S. precision airstrike targeting "a single dwelling in a wooded area

---

[43] *Id.* James Dever & John P. Dever Jr., *Making Waves: Refitting the* Caroline *Doctrine for the Twenty-First Century*, 31 QUINNIPIAC L. REV. 165, 174 (2013) (citing Daniel Webster, *Case of the* Caroline, NILES' NATIONAL REGISTER, Sept. 24, 1842, at 57) (detailing the history of the *Caroline* Doctrine).

[44] DOWDY ET AL., *supra* note 27, at 142.

[45] *Id.*

[46] *Id*. There are five LOAC principles: (1) military necessity; (2) distinction; (3) proportionality; (4) unnecessary suffering; and (5) honor. *Id.* at 137. In the above example, the conduct-based targets wearing civilian clothes violated the LOAC principle of distinction. *See id.* at 13

[47] *See* Mary Anne Weaver, *The Short, Violent Life of Abu Musab al-Zarqawi*, ATLANTIC (June 8, 2006), https://www.theatlantic.com/magazine/archive/2006/07/the-short-violent-life-of-abu-musab-al-zarqawi/304983/ [https://perma.cc/FU8Q-ZUYF].

[48] *See* Raffi Khatchadourian, *The Kill Company*, THE NEW YORKER (June 29, 2009), https://www.newyorker.com/magazine/2009/07/06/the-kill-company [https://perma.cc/3RAJ-WXNP] ("But most insurgent groups in Iraq don't wear uniforms, so their members must be "positively identified" by informants or other forms of intelligence before they can legally be killed. An insurgent is positively identified if there is "reasonable certainty" that he belongs to a declared hostile group.").

[49] Weaver, *supra* note 47. Al -Zarqawi's first beheading victim was an American engineer named Nicholas Berg; he was also the violent architect of numerous civilian bombings and infamously killed sixty wedding attendees in an Amman hotel. *Id.*

surrounded by very dense palm forest" killed al-Zarqawi alongside "his spiritual adviser and four other[s] including a woman and a child."[50]

Drone strike programs offer a prominent example of the conceptual challenges posed by applying traditional LOAC targeting standards to nonstate and terrorist actors.[51] Former State Department Legal Adviser Harold Hongju Koh remarked about the Predator drone program that the U.S. maintains lawful recourse to "lethal force . . . to defend itself . . . including by targeting persons such as high-level al Qaeda leaders who are planning attacks."[52] The remark appears innocuous yet it presupposes nonstate actors and terrorist organizations maintain tightly-affiliated top-down relationships when they often consciously do not. Might persons loosely affiliated with ISIS goals living in Manila, learning bomb-making tradecraft online, and counseling like-minded associates qualify as conduct-based targets?[53] To make the analogy even more attenuated, how about Manila ISIS sympathizers who are effective online ideologues and later credited as sources of inspiration by lone-wolf actors who targeted civilians?

III. FINANCIAL WARFARE

A. Little Flash, Big Bang

Conventional armed conflicts tend to conform to predictable patterns whereby combatants are deployed against fixed units.[54] Terrorism embraces unconventional tactics because it is a means to challenge stronger powers.[55] No universal definition of terrorism exists, although it is understood to have four key components: "(1) a violent act; (2) civilian victim(s); (3) the [terrorists] have a political, religious, or social motive; and (4) terrorists seek to provoke a political reaction and spread fear."[56] A peculiar feature of terrorism amongst transnational violence is that "one man's terrorist is another man's freedom

[50] John F. Burns, *U.S. Strike Hits Insurgent at Safehouse*, N.Y. TIMES (June 8, 2006), https://www.nytimes.com/2006/06/08/world/middleeast/08cnd-iraq.html [https://perma.cc/PN2D-GU9C].

[51] Waxman, *supra* note 34, at 447-51.

[52] Harold Hongju Koh, Former Legal Adviser, U.S. State Dep't., The Obama Admin. & Int'l. L.: Remarks at the Annual Meeting of the Am. Soc'y. of Int'l. L. (Mar. 25, 2010) [https://perma.cc/9X2J-9YDH]. For a discussion regarding drone targeting of U.S. persons, including dual U.S. and Yemini citizen Anwar al-Awlaki, see generally Martin S. Flaherty, *The Constitution Follows the Drone: Targeted Killings, Legal Constraints, and Judicial Safeguards*, 38 HARV. J.L. & PUB. POLICY 21, 22-24 (2015).

[53] *See* Waxman, *supra* note 34, at 447.

[54] JOHN ARQUILLA, INSURGENTS, RAIDERS, AND BANDITS: HOW MASTERS OF IRREGULAR WARFARE HAVE SHAPED OUR WORLD 3 (2011).

[55] *See* THOMAS RID & MARC HECKER, WAR 2.0: IRREGULAR WARFARE IN THE INFORMATION AGE vii (2009).

[56] Sahar F. Aziz, *The Authoritarianization of U.S. Counterterrorism*, 75 WASH. & LEE L. REV. 1573, 1586-87 (2018).

fighter," *i.e.*, terrorism is not inherently perceived as either criminal or illegitimate.[57] Indeed, there are certain sets of circumstances such as struggles for political voice or self-determination about which there is no consensus whether terrorist-type tactics are unlawful but excusable or unlawful yet justifiable or perhaps even lawful according to international norms.[58] These ambiguities and varying perspectives are why international law, in part, has not reached a universal definition of terrorism.[59]

In certain respects, terrorism is an ancient gambit and a modern manifestation of old wine in a new bottle.[60] It was first associated with the excesses of the French Revolution's "*regime de la terreur*" and evolved over a century to describe non-state actors applying their aptitude for subversion, disruption and anarchy to the controlling Russian and French governments of the late nineteenth century.[61] Following World War II, terrorists made headlines around the world by hijacking civilian aircraft.[62] In response, "[t]he international community enacted treaties" and increased airport security measures which, taken together, reduced the incidence of harm to passengers.[63] It was at this moment, the late 1960s and early 1970s, that terrorists relearned the valuable lesson of grabbing headlines, which was critical for the emergence of a new type of transnational terrorism.[64]

Generally, twenty-first century terrorism arises from a mix of religious fervor reinforced with political ideology and geopolitical goals.[65] The initial campaign against Al Qaeda following 9/11 "has morphed into transnational conflicts against various terrorist groups like the Islamic State of Iraq and [Syria (ISIS)] that did not exist in 2001."[66] This metastasized to pose a greater threat to society because terrorists are harder to deter; the relationship between the means employed and the goals are more attenuated; attacks are increasing in scale; and the proliferation and greater availability of weapons of mass destruction coupled

[57] *Id*. at 1585-86.

[58] *See* TED HONDERICH, AFTER THE TERROR 151, 170, 184-85 (2003).

[59] *See* NEIL BOISTER, AN INTRODUCTION TO TRANSNATIONAL CRIMINAL LAW 106-07 (2012).

[60] *See, e.g.,* Antoine Sottile, *Le Terrorisme International,* 65 RECUEIL DES COURS 89, 91 (1938) (remarking, during a lecture at the Academy of International Law at the Hague in 1938, that "The intensification of terrorist activity in the past few years has made terrorism one of today's most pressing problems.").

[61] Reuven Young, *Defining Terrorism: The Evolution of Terrorism as a Legal Concept in International Law and Its Influence on Definitions in Domestic Legislation*, 29 B.C. INTL. & COMP. L. REV. 23, 27-28 (2006).

[62] *Id.* at 28.

[63] *Id.*

[64] *Id*.

[65] *Id.*

[66] Trumbull, *supra* note 28, at 97.

with society's ever-increasing dependence on the cyber domain and electronic lifestyles.[67]

It is axiomatic that terrorist attacks do not require large amounts of money and their impact is disproportionate to their cost. 9/11 cost Al Qaeda approximately $500,000.[68] The cost to the U.S. was upwards of $3.3 trillion.[69] Put differently, al Qaeda received a $7 million return on investment for every dollar it spent planning and carrying out its attacks.[70] The cost in human life was far greater. On 9/11, 19 men hijacked four fuel-laden commercial jets bound for West Coast destinations. 2,753 people lost their lives in Manhattan when American Airlines Flight 11 and United Airlines Flight 175 crashed into the Twin Towers.[71] 184 people died when American Airlines Flight 77 crashed into the Pentagon and 40 more people were killed aboard United Airlines Flight 93 when the plane crashed into a field near Shanksville, Pennsylvania.[72] For the U.S. military, Operations Enduring Freedom, Iraqi Freedom, New Dawn, Inherent Resolve, and Freedom's Sentinel resulted in 6,978 U.S. casualties.[73]

B. Funding Terror

Terrorist groups like "ISIS, al Qaeda, Hezbollah, and Boko Haram rely upon vast networks of money moving around the world" to finance their ideologies.[74] Without this extensive network of funding, most terrorist organizations would be unable to launch attacks or find the impact of their attacks blunted.[75] Khalid Sheik Mohammed, "the principle architect of the 9/11 attacks," used wire transfers and funds that were delivered to the U.S. or deposited abroad and then accessed from within the U.S.[76] His nephew, Ali Abdul Aziz Ali, aided the 9/11 terrorists by wiring $114,500 to the U.S. that was utilized by an associated cell

---

[67] *See* Young, *supra* note 61, at 28-29.

[68] *9/11 Panel: al Qaeda Planned to Hijack 10 Planes*, CNN (June 17, 2004), http://www.cnn.com/2004/ALLPOLITICS/06/16/911.commission/ [https://perma.cc/DP3T-GLP6].

[69] Kimberly Amadeo, *How the 9/11 Attacks Affect the Economy Today*, BALANCE (Nov. 6, 2018), https://www.thebalance.com/how-the-9-11-attacks-still-affect-the-economy-today-3305536 [https://perma.cc/C38M-G4NK].

[70] *See id.*

[71] *September 11 Terror Attacks Fast Facts*, CNN (Sept. 3, 2018), https://www.cnn.com/2013/07/27/us/september-11-anniversary-fast-facts/index.html [https://perma.cc/4ZKJ-GWYE].

[72] *Id.*

[73] *Casualty Status*, U.S. DEP'T OF DEF. (Dec. 29, 2018), https://dod.defense.gov/News/Casualty-Status/ [https://perma.cc/V8ZD-V2PE].

[74] Roy G. Dixon III, *The New York Department of Financial Service's New Anti-Money Laundering Regulation: A Model for Improvement*, 21 N.C. BANKING INST. 383, 383 (2017).

[75] *Id. See also* MICHAEL FREEMAN, INTRODUCTION TO FINANCING TERRORISM: CASE STUDIES 3 (Michael Freeman ed., 2012).

[76] 9/11 COMM'N REP., NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 145 (2004).

in Hamburg, Germany to pay for flight training.[77] Aziz sent multiple "bank-to-bank transfers –including transactions for $10,000, $20,000, and $70,000–to bank accounts at SunTrust Bank in Florida."[78] The transaction amounts to SunTrust are notable because, pursuant to the Bank Secrecy Act of 1970,[79] the bank was required to report Customer Transaction Reports ("CTRs") above $10,000 to the Treasury Department's Financial Crimes Enforcement Network ("FinCEN") and file a Suspicious Activity Report ("SAR") for any wire transfer they deemed suspicious.[80] Tragically, SunTrust never filed a SAR in connection with the 9/11 attacks and indeed no financial institution filed a SAR in connection with any of the 19 hijackers' transactions before 9/11.[81]

Terrorist organizations go about raising money in different ways; some rely on criminal activity whereas others acquire revenue from private donations from interested persons or groups.[82] They do so because"[f]inancing is required not only to fund specific missions but to meet the broader organizational costs of developing and maintaining a terrorist organization and to create an enabling environment necessary to sustain their activities."[83] While the direct cost of mounting specific attacks is alarmingly low, it does cost money to maintain a terrorist network, enable recruitment, sustain terror cells, and fund planning and procurement between attacks.[84] Further, terror groups require funds "to finance the ostensibly legitimate activities required to provide a veil of legitimacy for their organizations."[85] As a result, "[d]isrupting terrorist financing involves both systemic safeguards, which protect financial systems from abuse, and targeted economic sanctions informed by counterterrorism intelligence."[86]

---

[77] *Id.* at 224. According to the 9/11 Commission Report, Ali was not required to provide identification when making these transfers, nor were the aliases that he chose questioned about their authenticity or validity. *Id.*

[78] Nicholas Ryder, *Is It Time to Reform the Counter-Terrorist Financing Reporting Obligations? On the EU and the UK System*, 19 GERMAN L.J. 1169, 1171 (2018).

[79] 31 U.S.C. § 5311 (2012); *Senate Hearing on Foreign Bank Secrecy: Hearings Before the Subcomm. on Fin. Inst. of the Comm. on Banking and Currency*, 91st Cong. 170 (1970) (statement of Eugene Rossides, Former Assistant Secretary, Treasury for Enforcement and Operations), https://www.fincen.gov/sites/default/files/shared/FincenOurStory.pdf [https://perma.cc/TRX6-75EW]. (explaining that the BSA was not meant to defeat terrorist financing but was instead introduced to "build a system to combat organized crime and white-collar crime and to deter and prevent the use of secret foreign bank accounts for tax fraud.").

[80] Ryder, *supra* note 78, at 1171.

[81] *Id*. at 1171-72.

[82] FIN. ACTION TASK FORCE, ORG. FOR ECON. COOPERATION & DEV. [OECD], TERRORIST FINANCING 4 (2008), http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf [https://perma.cc/NG8Q-86GU].

[83] *Id.*

[84] *Id.*

[85] *Id.*

[86] *Id.*

Terror groups exploit a number of loopholes in the current system to maintain a flow of money through legitimate sources.[87] Generally, the sources of terrorist finance can be divided into two types: "financing *from above*, [where] large-scale financial support is aggregated centrally by states, companies, charities or permissive financial institutions; and financing *from below*, in which" terror groups fundraise using small-scale and dispersed sources based on, for instance, "self-financing by the terrorists themselves using employment or welfare payments."[88] Common methods include creating "offshore shell companies, front organizations, or trusts to receive money; transferring funds from the bank accounts of charitable and non-profit organizations under the guise of a 'gift;' and [purchasing] real estate and art to conceal [money sources]."[89] Additionally, transfers using banks are smaller in size in an attempt to "limit exposure and avoid detection [which] may later be combined with other deposits for financing purposes."[90] "Money launderers [that] use small-scale transfers to structure deposits [may then] evade the reporting thresholds for Customer Transaction Reports ('CTR') and Suspicious Activity Reports ('SAR')."[91]

C. Disrupt to Protect

President Bush declared the "War on Terror" on September 20, 2001.[92] Four days later, he instigated the "Financial War on Terror" when he said the U.S. "will starve terrorists of funding, turn them against each other, rout them out of their safe hiding places, and bring them to justice."[93] President Bush made an explicit connection between stopping terrorist financing and preventing real-world attacks on Americans when he said "[m]oney is the lifeblood of terrorist organizations."[94] His announcement was followed by frequent declarations — notably from David D. Aufhauser, General Counsel to the U.S. Department of

---

[87] *Id*. at 11.

[88] *Id.*

[89] Dixon, *supra* note 74, at 384 (2017). For further discussion regarding a number of different complex money laundering mechanisms terrorist organization carry out, see PETER REUTER, CHASING DIRTY MONEY: THE FIGHT AGAINST MONEY LAUNDERING 27-33 (2004).

[90] Dixon, *supra* note 74, at 385.

[91] *Id.* "CTRs [necessitate] reporting of 'currency transactions' over $10,000, while SARs [mandate] reporting of transactions over $5,000" that might involve money laundering or BSA violations. *Id.*

[92] NICHOLAS RYDER, THE FINANCIAL WAR ON TERRORISM: A REVIEW OF COUNTER-TERRORIST FINANCING STRATEGIES SINCE 2001 2 (2015).

[93] *Id.* at 1171. Prior to 9/11, terrorist financing had received limited attention in a number of academic studies and the evolution of U.S. AML regulation can be traced in chronological order: the Bank the Bank Secrecy Act of 1970, the Racketeer Influence and Corrupt Organization Act of 1970, the Money Laundering Control Act of 1986, the Annunzio-Wylie Anti-Money Laundering Act of 1992, and the USA Patriot Act of 2001. *Id.* at 1172.

[94] Press Release, Off. of Press Secretary, President Freezes Terrorists' Assets (Sept. 24, 2001), https://georgewbush-whitehouse.archives. gov/news/releases/2001/09/20010924-4.html [https://perma.cc/Y9UK-QDHN].

the Treasury — calling for more efforts aimed at freezing terrorist funding sources.[95] In his testimony before the Senate Judiciary Committee, Aufhauser explained that on 9/11 he was at an international money laundering conference in Cambridge, Massachusetts, in which there was a lot of self-congratulations on current efforts to curb money laundering.[96] However, when the entire conference watched the World Trade Center buildings collapse, Aufhauser explained that:

> It was . . . the realization that the gathering had been looking, for too long, at the world through the wrong end of a telescope. Money had been spirited around the globe by means and measures and in denominations that mocked detection. The most serious threat to our well-being was now clean money intended to kill, not dirty money seeking a place of hiding.[97]

"Terrorist groups and criminal networks share many of the same characteristics, including methods and sources of finance."[98] In 2011, Yury Fedotov, the Executive Director of the United Nations Office on Drugs and Crime, remarked "criminal profits from drug trafficking, transnational organized crime, and money laundering represent an increasing share of terrorist finance."[99] Prior to 9/11, the U.S. government lacked the know-how to stop terrorist financing.[100] When the Central Intelligence Agency ("CIA") was admonished for its lack of information on al-Qaeda's finances pre-9/11, its lackluster response was "terrorist financing [is] an extraordinarily hard target."[101] Indeed, the U.S. had "considered it futile to monitor al Qaeda's money

---

[95] David Aufhauser, *Testimony of David D. Aufhauser General Counsel U.S. Department of the Treasury Before the Senate Judiciary Committee Washington, D.C.,* U.S. DEPT' OF THE TREASURY (Nov. 20, 2002), https://www.treasury.gov/press-center/press-releases/Pages/po3639.aspx [https://perma.cc/9WH9-98UL]

[96] *Id. See also An Assessment of the Tools Needed to Fight the Financing of Terrorism, Hearing Before the Sen. Comm. on the Judiciary*, 107th Cong. 17 (Nov. 20, 2002) (statement of David Aufhauser, Gen. Couns., Dep't of the Treasury, Washington, D.C.).

[97] Aufhauser, *supra* note 95. In addition to America that has suffered disastrous consequences for its lacks of a robust CFT scheme, the E.U. is also facing its second decade of intense transnational terrorist attacks. Ryder, *supra* note 92, at 1170. In the past three years, terrorists struck in France, Belgium, Germany, Sweden, Spain, Turkey, the United Kingdom, Finland, and Russia; moreover, their tactics all evince sophisticated terrorist support networks and inexpensive acts of terrorism. *Id.*

[98] Yusef Al-Jarani, *A War Developing Countries Cannot (Afford to) Win*, 35 YALE L. & POLICY REV. 585, 586 (2017). It is important to not overly stretch the degree of similarity; modern terrorists rely increasingly on donations and self-financing to avoid the formal financial institutions most affected and regulated by AML legislation. *Id.* at 601.

[99] *Id.* at 586.

[100] *Id.* at 588.

[101] JOHN ROTH, DOUGLAS GREENBURG & SERENA WILLE, NAT'L COMMISSION ON TERRORIST ATTACKS UPON THE U.S., MONOGRAPH ON TERRORIST FINANCING: STAFF REPORT TO THE COMMISSION 35 (2004),

trail because of the erroneous belief Osama bin Laden, through his personal fortune, financed all of the organization's operations."[102] The CIA was not the only government body that failed to properly examine Al Qaeda's terrorist financing pre-9/11.[103] Issued just ten days before the 9/11 attacks, the Treasury Department's 2001 National Money Laundering Strategy was primarily concerned with drug trafficking and high-level international fraud and did not devote any attention to terrorist financing.[104]

As a result of the U.S. government failing to actively concern itself with terrorist financing, it was unprepared for post-9/11 realities.[105] In a certain sense, financial warfare is not a new concept for the U.S. government; the U.S. first codified presidential authority to employ economic sanctions against foreign countries in 1917 in the Trading with the Enemy Act ("TWEA").[106] Some decades later the U.S. created the Treasury Department's "Office of Foreign Assets Control (OFAC) to target Chinese assets during the Korean Conflict."[107] 9/11 was a watershed moment, however, and exigencies necessitated creative measures to halt terrorist financing. Two weeks after the attacks, President Bush issued Executive Order 13224 ("E.O. 13224") which froze the assets of twenty-seven individuals and organizations.[108] E.O. 13224 "centered on two goals: stopping the flow of money to al Qaeda and convincing the public that something was being done."[109] E.O. 13224 declared a national emergency and allowed President Bush to use the powers of the International Emergency Economic Powers Act ("IEEPA").[110] Using this power under IEEPA, President Bush authorized the Treasury Department "to freeze the assets of foreign and domestic organizations within [U.S. jurisdiction], including assets of financial

http://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf [https://perma.cc/BQ38-GPRL].

[102] Justin Santolli, Note, *The Terrorist Finance Tracking Program: Illuminating the Shortcomings of the European Union's Antiquated Data Privacy Directive*, 40 GEO. WASH. INTL. L. REV. 553, 556 (2008).

[103] *See* Al-Jarani, *supra* note 98, at 588.

[104] Santolli, *supra* note 102, at 556.

[105] *See id.*

[106] Chris Jones, *Caught in the Crosshairs: Developing A Fourth Amendment Framework for Financial Warfare*, 68 STAN. L. REV. 683, 689 (2016). *See generally* Trading with the Enemy Act, Pub. L. No. 65-91, §5(b), 40 Stat. 411, 415 (1917).

[107] Jones, *supra* note 106, at 689.

[108] Exec. Order No. 13,224, 66 Fed. Reg. 49,079 (Sept. 23, 2001); Jones, *supra* note 106, at 691.

[109] Laura K. Donohue, *Anti-Terrorist Finance in the United Kingdom and United States*, 27 MICH. J. INTL. L. 303, 378 (2006).

[110] International Emergency Economic Powers Act, 50 U.S.C. § 1702(a)(1)(B) (2000). The International Emergency Economic Powers Act empowers the President to designate individuals or organizations as national security threats, prohibit or regulate transactions involving those designated individuals, freeze and seize their assets, and make it a crime to materially assist the named individuals and groups. 50 U.S.C. § 1702(a)(1)(A)-(B).

institutions."[111] Bush gave the Treasury Department this power to "avoid not just criminal law but the judicial system altogether in [his administration's] efforts to prevent the flow of funds."[112] The most famous initiative to combat terrorism was the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("PATRIOT Act").[113] Title III of the PATRIOT Act sets forth the regulations concerning countering terrorist financing ("CFT").[114] The Act strengthened the executive branch's ability to freeze and seize assets, broadened the President's power under the IEEPA, and expanded U.S. extraterritorial jurisdiction.[115]

The PATRIOT Act was so revolutionary in certain respects that David Aufhauser described Title III as "'the smart bomb of terrorist financing.'"[116] Amongst the Act's most significant measures was its requirement that "banks, savings associations, credit unions, securities broker-dealers, mutual funds, futures commission merchants, and introducing brokers enhance their customer identification measures."[117] All U.S. financial institutions were required to maintain anti-money laundering ("AML") programs.[118] Additionally, the Act expanded the number of entities required to file SARs: "[w]here before the Bank Secrecy Act of 1970 required banks and credit unions to report $10,000 or more in cash transfers, now 'any person who is engaged in a trade or business' that received more than $10,000 in cash must file an SAR."[119]

Despite the PATRIOT Act's broad scope, some critics maintained that it was a "hastily assembled" version of existing AML legislation from the 1980s and 1990s originally intended to combat drug cartels and enterprise crime.[120] For

---

[111] Santolli, *supra* note 102, at 558.

[112] *Id.* (quoting Donohue, *supra* note 109, at 307).

[113] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT") Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[114] *Id.* §§ 301-03.

[115] Santolli, *supra* note 102, at 558.

[116] *Id.* (quoting *Terrorism: Growing Wahhabi Influence in the Unite*d *States: Hearing Before the Subcomm. on Terrorism, Tech. and Homeland Sec. of the H. Comm. on the Judiciary*, 108th Cong. 67-80 (2003) (statement of David D. Aufhauser, General Counsel, Dep't of the Treasury)).

[117] Donohue, *supra* note 109, at 372.

[118] Jeffrey P. Taft & Christine Poulon, *Compliance Obligations and Enforcement Actions Under the USA Patriot Act*, 60 CONSUMER FIN. L.Q. REP. 316, 317-18 (2006).

[119] Donohue, *supra* note 109, at 372.

[120] Richard J. Maiman, *Lobbying for Rights During the 'War on Terror': The American Civil Liberties Union After 9/11, in* STRATEGIC VISIONS FOR HUMAN RIGHTS: ESSAYS IN HONOUR OF PROFESSOR KEVIN BOYLE 126-40 (Geoff Gilbert et al. eds., 2010). The Treasury Department defines "money laundering" as the process of making proceeds derived from criminal activity appear clean. *History of Anti-Money Laundering Laws*, U.S. DEP'T TREASURY FIN CRIMES ENFORCEMENT NETWORK, https://www.fincen.gov/history-anti-money-laundering-laws [http://perma.cc/7CNY-R69F] (last visited Feb. 25, 2019). Money

years afterward, detractors maintained "[t]he dirty little secret behind efforts to stem terrorist finance in the . . . United States is that, to date, such initiatives have been spectacularly unsuccessful in making a significant dent in terrorist operations."[121] In truth, the "strategic revelation of post-9/11 warfare is the 'revolutionary' idea that banks are the 'prime movers' in the twenty-first century financial and commercial environment."[122] Consequently, "the government instead 'relie[s] more and more on the ability of financial institutions to act as protective gatekeepers to the financial system by identifying, reporting, and preventing' impermissible use of the financial system."[123] Put differently, the PATRIOT Act "shifted much of the burden of enforcing sanctions [from the government] to the private sector."[124]

D. International Efforts

The U.S. "spends more on its defense budget than the next eight states combined but it [does not] go after terrorist finance on its own,"[125] since it requires assistance from the international community.[126] From a global perspective, the creation of a comprehensive AML/CFT strategy was "drawn from the idea that cutting off terrorist funds could slow down, disturb, and dismantle terrorist networks."[127] To implement this strategy, "two international organizations—namely, the United Nations and the Financial Action Task Force (FATF) created and perpetuate[d] a system of measures to prohibit acts of financing, freeze terrorist funds, and track down terrorists."[128] After 9/11, "substantial efforts [were] made to assure that countries [had] adopted and implemented laws consistent with these measures."[129] Nonetheless, these programs receive scant attention relative to their importance and there continues

laundering "is typically a three-step process: (i) placement—the launderer puts criminally-derived money into a legitimate enterprise; (ii) layering—the launderer places the money in . . . pretextual transactions to obfuscate the original source; and (iii) integration—the launderer [changes] the funds into non-cash instruments" like bank notes and letters of credit to finance criminal activities. Brittany Yantis et. al., *Money Laundering*, 55 AM. CRIM. L. REV. 1469, 1470 (2018).

[121] Donohue, *supra* note 109, at 390. *See also generally* Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended at 12 U.S.C. §§ 1724, 1813 (2012) and 15 U.S.C. § 78(a) (2012)).

[122] Jones, *supra* note 106, at 696 (quoting JUAN C. ZARATE, TREASURY'S WAR: THE UNLEASHING OF A NEW ERA OF FINANCIAL WARFARE 151 (2013)).

[123] *Id.* (quoting Juan C. Zarate, *Harnessing the Financial Furies: Smart Financial Power and National Security*, WASH. Q., Oct. 2009, at 43, 49).

[124] *Id*.

[125] Donohue, *supra* note 109, at 380.

[126] *Id*.

[127] Hamed Tofangsaz, *Criminalization of Terrorist Financing: From Theory to Practice*, 21 NEW CRIM. L. REV. 57, 58 (2018).

[128] *Id.*

[129] *Id.*

to be "little debate about whether the programs are proportionate to their potential effectiveness."[130]

Created in 1989, the FATF is an international organization whose mission includes "combating money laundering, terrorist financing and other related threats to the integrity of the international financial system."[131] In the wake of 9/11, the FATF expanded its objectives to include CFT.[132] A primary mechanism by which the FATF seeks to accomplish its goals is by having its members implement "Recommendations" which do not have the force of law although "failure to implement them is grounds for expulsion from the organization."[133] Despite their soft-law nature, Recommendations hold significant sway because countries do not want to be excluded from the FATF.[134] On the contrary, nations blacklisted by the FATF for non-compliance understand there can be significant consequences. In February 2018, the U.S. urged the FATF to place Pakistan, which was on the non-compliant list from 2012 to 2015, on notice it was again violating CFT standards.[135] Pakistan was apprehensive that the move would further isolate the country from the global community, damage its weak economy, cripple its banking sector and hinder its access to international markets.[136] Consequently, Pakistan scrambled in recent months to get back into compliance.[137] Audited by a FATF delegation in October 2018, the activities of Pakistan's non-profit organizations, brokerage houses, exchange companies and donations of corporate entities were laid bare and found wanting.[138] The delegation further noted shortcomings in Pakistan's commodity

[130] *Id.*

[131] *Who We Are*, FIN. ACTION TASK FORCE, http://www.fatf-gafi.org/about/ [http://perma.cc/72EL-XAFR] (last visited Feb. 25, 2019). Post-9/11, the FATF expanded its mission to include combating terrorist financing. *See History of the FATF*, FIN. ACTION TASK FORCE, http://www.fatf-gafi.org/about/historyofthefatf/ [http://perma.cc/5QRN-Z9MR] (last visited Feb. 25, 2019).

[132] *History of the FATF*, *supra* note 131.

[133] Laurel S. Terry, *U.S. Legal Profession Efforts to Combat Money Laundering and Terrorist Financing*, 59 N.Y.L. SCH. L. REV. 487, 518 (2015); *see also FATF Membership Policy,* FIN. ACTION TASK FORCE (Feb. 29, 2008) [http://perma.cc/93MX-975W].

[134] Terry, *supra* note 133, at 490.

[135] Salman Masood, *At U.S. Urging, Pakistan To Be Placed on Terrorism-Financing List*, N.Y. TIMES (Feb. 23, 2018), https://www.nytimes.com/2018/02/23/world/asia/pakistan-terror-finance-list.html [https://perma.cc/K2Z8-MCNB].

[136] *Id.*

[137] *FATF Team Not Happy With Pakistan's Efforts To Combat Terror Financing*, PRESS TRUST OF INDIA (Oct. 11, 2018), http://www.ptinews.com/news/10103186_FAFT-team-not-happy-with-Pakistan—s-efforts-to-combat-terror-financing—Report [https://perma.cc/V29J-DFAH].

[138] *Id.* The FATF auditing team was comprised of experts from the U.S., Indonesia, China, the UK, Maldives, and Turkey. *Id.* Being placed on FATF's blacklist could lead to serious problems for Pakistan because its banking system will be regarded by the international community as lacking proper AML/CFT controls. *Id.*

trading sector and an ineffective AML framework that failed to provide cross-verification of service providers.[139] Pakistan's compliance deadline is September 2019 and part of its 10-point action plan includes requiring government agencies to be able to handle foreign requests to aid CFT policies, freeze illegal assets, and strengthen extradition laws for those involved in terror financing and money laundering upon sufficient showing from other FATF member nations.[140]

In 2005, the UN Secretary-General established the Counter-Terrorism Implementation Task Force ("CTITF") to implement coordination and coherence in counter-terrorism efforts among its member states.[141] Pursuant to CTITF guidelines, "[t]errorism financing incorporates the distinct activities of fund-raising, storing and concealing funds, using funds to sustain terrorist organizations and infrastructure, and transferring funds to support or carry out specific terrorist attacks."[142] "Money laundering and terrorist financing are characterized by somewhat opposing dynamics and objectives."[143] Money laundering's goal is to eradicate the illicit origin of funds to prevent actors from enjoying the profits of their predicate crimes.[144] Terrorist financing implies "money dirtying," which is the reverse of money laundering.[145] In other words, terrorist financing aims to divert "clean money" into terrorist activities while money launderers want to conceal the origin of "dirty money."[146] Notwithstanding differences, domestic and international law tend to construe these activities in a similar light and the policy decision is often girded by arguments of rationality and efficiency.[147] Effective strategies against both terrorist financing and money laundering necessitate a "'horizontal strategy' embracing a wide variety of fields, including criminal law, administrative law, and . . . international law."[148] Moreover, terrorist financing and money laundering presuppose the deployment of financial institutions for illicit

[139] *Id.*

[140] *Id.*

[141] U.N. Counter-Terrorism Implementation Task Force, *CTITF Working Group Report: Tackling the Financing of Terrorism*, ii (Oct. 2009), http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_financing_eng_final.pdf [https://perma.cc/2MSH-UEK3].

[142] *Id.* at 3.

[143] Leonardo Borlini & Francesco Montanaro, *The Evolution of the EU Law Against Criminal Finance: the "Hardening" of FATF Standards Within the EU*, 48 GEO. J. INT'L. L. 1009, 1017 (2017).

[144] *See id.*

[145] BRIGITTE UNGER, *Money Laundering Regulation: From Al Capone to Al Qaeda, in* RESEARCH HANDBOOK ON MONEY LAUNDERING 19, 21 (Brigitte Unger & Daan van der Linde eds., 2013).

[146] Leonardo Borlini, *Regulating Criminal Finance in the EU in the Light of the International Instruments*, 36 Y.B. EUR. L. 553, 556-557 (2017).

[147] Borlini & Montanaro, *supra* note 143, at 1017.

[148] *Id.* at 1017-18.

purposes and often adopt similar techniques.[149] Finally, money laundering can be of singular importance in concealing the illegal origin and destination of funds directed to finance terrorist activities.[150] For these reasons, combining AML/CFT strategies is usually good policy. For example, the Money Laundering Control Act makes it a crime to knowingly "conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or . . . to avoid a transaction reporting requirement under State or Federal law."[151] Further, many "federal agencies investigate cases of suspected money laundering and terrorist financing, including the Financial Crimes Enforcement Network, Federal Bureau of Investigation, Department of Justice, Securities and Exchange Commission, and Immigration and Customs Enforcement."[152]

IV. CYBER DOMAIN ISSUES

A. Unwarranted Optimism

In October 2018, the White House released its National Strategy for Counterterrorism.[153] Per the document:

> The technological advances of the past century have created an interconnected world. . . . Terrorists use the . . . same publicly available technologies to command and control their organizations and to plot attacks . . . and abuse the global financial system to raise funds and procure weapons, materiaEL, and basic necessities.[154]

---

[149] PAUL ALLAN SHCOTT, REFERENCE GUIDE TO ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM I-5-I-10 (2d ed. Supp. 2006).

[150] UNGER, *supra* note 145, at 20-21. *See also, e.g.*, S.C. Res. 1333 (Dec. 19, 2000) (noting that the Taliban gained illegal monies by trafficking opium and taxing the drug trade in areas under its control, and these funds were subsequently used to support terrorist organizations). According to the U.N. Office for Drug Control and Crime Prevention, estimates of the Taliban's drug income range from $15 to $27 million per year. *See* Rep. of the Committee of Experts Appointed Pursuant to Security Council Resolution 1333 (2000), ¶ 15(a), Regarding Monitoring of the Arms Embargo against the Taliban and the Closure of Terrorist Training Camps in the Taliban-held Areas of Afghanistan, ¶ 60, U.N. Doc. S/2001/511 (May 21, 2001). Similarly, Resolution 2199, adopted by the UN Security Council on February 12, 2015, underscores the possibility terrorism is funded by the proceeds of organized crime and drug trafficking. *See* S.C. Res. 2199, ¶ 8 (Feb. 12, 2015). For continued reading, see Borlini & Montanaro, *supra* note 143, at 1017-18.

[151] 18 U.S.C. § 1956(a)(1)(B)(i)-(ii) (2012); Terry, *supra* note 133, at 498.

[152] Terry, *supra* note 133, at 498.

[153] THE WHITE HOUSE, NATIONAL STRATEGY FOR COUNTERTERRORISM OF THE UNITED STATES OF AMERICA (Oct. 2018), https://www.dni.gov/files/NCTC/documents/news_documents/NSCT.pdf [https://perma.cc/W8TE-LBSV].

[154] *Id.* at 15.

Just a month prior, the White House published its National Cyber Strategy.[155] Under a subheading titled *Attribute and Deter Unacceptable Behavior in Cyberspace,* the government asserted:

> All instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States. This includes . . . public attribution. . . . The United States will formalize and make routine how we work with like-minded partners to attribute and deter malicious cyber activities.[156]

Yet aside from the saber-rattling found within the strategies, the truth is that U.S. responses to cyber events remain effete. The consequences of non-action are staggering. In 2012, former National Security Agency ("NSA") director General Keith Alexander declared that the loss of value due to cyber espionage in the U.S. amounted to the "greatest transfer of wealth in world history."[157] In February 2018, the Trump Administration Council of Economic Advisers published its report on the cost of malicious cyber activity to the U.S. economy which was estimated to be $57 billion to $109 billion in 2016.[158] The Council was especially concerned with attacks on Critical Infrastructure ("CI"), which is necessary to the smooth functioning of the U.S. economy and in particular the financial sector. [159] The Council warned that "[a]ttacks on the financial sector can reduce confidence in the financial system and affect a great number of public and private entities. . . . In recent years, certain aspects of the global financial system have proven to be vulnerable to cyber threats."[160] The Council asserted

---

[155] THE WHITE HOUSE, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA (Sept. 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [https://perma.cc/AL42-5C5V].

[156] *Id.* at 21.

[157] Josh Rogin, *NSA Chief: Cybercrime Constitutes the "Greatest Transfer of Wealth in History*, FOREIGN POLICY (July 9, 2012), https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/ [https://perma.cc/8FG9-3TZA].

[158] COUNCIL OF ECON. ADVISERS, EXEC. OFFICE OF THE PRESIDENT, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 1 (Feb. 2018), https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf [https://perma.cc/8M5T-W9Y5].

[159] *Id.* CI refers to the facilities, systems, and networks that crucial to the functioning of a nation. CI involves multiple sectors including agriculture, energy, health, and financial systems. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-09-654R, THE DEPARTMENT OF HOMELAND SECURITY'S (DHS) CRITICAL INFRASTRUCTURE PROTECTION COST-BENEFIT REPORT 1 (2009), https://www.gao.gov/assets/100/96236.pdf [https://perma.cc/4HKL-LQRE]. President Obama in 2009 declared CI to be a "strategic national asset." Press Release, Off. of the Press Secretary*, Remarks by the President on Securing our Nation's Cyber Infrastructure,* THE WHITE HOUSE (May 29, 2009), https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure [https://perma.cc/5DT7-Q64Q].

[160] COUNCIL OF ECON. ADVISERS, *supra* note 158, at 37.

that since the disclosure of the Bank of Bangladesh theft,[161] a number of similar robberies have come to light, stating that "in 2015 hackers used stolen SWIFT credentials to successfully transfer over $12 million . . . owned by Banco Del Austro [and] over $60 million was stolen from the Taiwanese Far Eastern International Bank."[162]

During his March 2018 congressional nomination hearing to become NSA Director and Commanding General of U.S. Cyber Command, then-Lieutenant General Paul Nakasone quipped "[t]hey don't think . . . much will happen" in response to Senator Dan Sullivan's question regarding what China, Russia, North Korea, and Iran expect when they launch cyber operations against the U.S.[163] A significant portion of the problem lies in an inability to identify the perpetrator.[164] This so-called "attribution problem" has, in part, frustrated efforts to create international treaties to regulate malicious cyber activity.[165] "As others have noted, '[a]ttribution of a cyber-attack to a state is a, if not the, key element in building' a decisive cyber strategy."[166] Notwithstanding the technological impediments to attribution, the real impediments are the difficult policy decisions and legal issues states must navigate to obtain a functioning cyber-deterrence system.[167]

---

[161] *See* discussion *infra* Section V.

[162] COUNCIL OF ECON. ADVISERS, *supra* note 158, at 38. In 2006, the Treasury Department and the CIA collaborated on the Terrorist Finance Tracking Program (TFTP) but data privacy protection initiatives by the E.U. members obviated much of TFTP's potential. Justin Santolli, *The Terrorist Finance Tracking Program: Illuminating the Shortcomings of the European Union's Antiquated Data Privacy Directive*, 40 GEO. WASH. INTL. L. REV. 553, 555, 573-74, 581 (2008).

[163] Ellen Nakashima, *Incoming NSA Chief has a reputation for winning 'all the important fights.' Russia will be his biggest test yet*, WASH. POST (Apr. 1, 2018), https://www.washingtonpost.com/world/national-security/incoming-nsa-chief-has-a-reputation-for-winning-all-the-important-fights-russia-will-be-his-biggest-test-yet/2018/03/31/ee943ef0-23d6-11e8-badd-7c9f29a55815_story.html?noredirect=on&utm_term=.6a498eb9eb02 [https://perma.cc/7AK8-HYGP].

[164] COUNCIL OF ECON. ADVISERS, *supra* note 158 at 4, 7.

[165] Delbert Tran, *The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack*, 20 YALE J. L. & TECH. 376, 383 (2018).

[166] *Id.* at 384 (quoting Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 191, 232 (2009)). Cyber attribution is hard for multiple reasons: (1) the architecture of the internet and the nature of data transmission across networks complicates attribution efforts; (2) users may employ tactics to obfuscate their online activity; (3) even presupposing the internet could be redesigned to authenticate each IP address of every scintilla of data sent over networks, these addresses would simply identify the machine source and not the person manipulating the system; (4) even if all the technological problems are overcome, there remains the issue whether a state may be held responsible for an individual's actions. *Id.* at 387, 389-90.

[167] David Wallace, Shane Reeves & Trent Powell, *Revisiting Belligerent Reprisals in the Age of Cyber*, 102 MARQ. L. REV. 81, 101-02 (2018).

B. Multiplying Threat-Vectors

The cyber domain may appear "bewildering . . . its infrastructure is shared [amongst] civilians and militaries, governments and businesses" malicious pre-written code may be deployed with a single click; non-state actors can be equally as powerful as some states; "and it can be difficult to identify transgressors, both because the source of [cyber events] can be masked and because states often operate through non-state [intermediaries]."[168]

"Cyberattacks have increased in [power] and sophistication to the [point] they are now a threat to global stability."[169] In 2017, a study of 254 domestic and transnational companies estimated "the annual cost of responding to cyberattacks at $15.3 million per company, a 27.4 percent increase from 2016."[170] Per the World Economic Forum's Global Risk Report for 2018, these increases show "'a growing trend of using cyberattacks to target critical infrastructure and strategic industrial sectors, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning."[171] "Cybersecurity concerns that were once primarily about data security . . . are now concerns about human safety and the operational preservation of industrial and financial infrastructure."[172] In today's world, cyber-physical systems, commonly dubbed the Internet of Things ("IoT"), "are not only potential targets, but also attack vectors from which to launch new types of cyber disruptions."[173] The FBI recently issued a cyber alert reinforcing what experts said about the exponential explosion of threat vectors due to the IoT because "the IoT is essentially, inherently chronically insecure and wide open to potentially devastating cyber attacks that could have far-reaching national and . . . international consequences for vital networks and systems."[174]

---

[168] Rebecca Crootof, *International Cybertorts: Expanding State Accountability in Cyberspace*, 103 CORNELL L. REV. 565, 644 (2018). Mass killings in the U.S. like the 2009 Fort Hood shooting; the 2015 Garland, Texas redux of the French Charlie Hebdo attack; and the 2015 San Bernardino shooting are examples of how the internet promotes radicalization. *See* Susan Klein & Crystal Flinn, *Social Media Compliance Programs and the War Against Terrorism*, 8 HARV. NAT'L SEC. J. 53, 61 (2017).

[169] Henry Kenyon, *Report: Global Systems Threatened by Increased Cyberattacks*, CQ ROLL CALL, June 29, 2018, 2018 WL 3194812.

[170] *Id.*

[171] *Id.* (quoting WORLD ECON. FORUM, THE GLOBAL RISKS REPORT 2018 15 (2018)).

[172] Laura DeNardis & Mark Raymond, *The Internet of Things As A Global Policy Frontier*, 51 U. CAL. DAVIS L. REV. 475, 475 (2017).

[173] *Id.* at 476.

[174] Martyn Warwick, *FBI Warns of 'Devastating' Cyberattacks on IOT Networks*, TELECOM TV (Aug. 7, 2018), https://www.telecomtv.com/content/security/fbi-warns-about-potentially-devastating-cyber-attacks-on-iot-networks-31941/ [https://perma.cc/MS2J-7WYF].

C. Public-Private Information Sharing

As John Chung has argued:

> A basic challenge in cybersecurity is the fact almost eighty-five percent of America's CI is owned by the private sector. . . . CI systems are [therefore] owned and operated by [a myriad of] businesses, which in turn may have thousands more private entities who . . . supply, service, or access the CI systems. The national cybersecurity framework [published by the National Institute of Standards and Technology ("NIST")] relies on private actors to invest in a sufficient amount of cybersecurity measures to [mitigate or] avoid catastrophic damage to CI.[175] However . . . [t]he government does not impose [a security regime on the private sector], leaving it to the private-sector entities to set their own practices and policies for protecting their computer systems.[176]

Further, "[o]n February 18, 2013 the private cybersecurity firm Mandiant [released] a report on a group it [dubbed] Advanced Persistent Threat 1 (APT1) that had purportedly breached almost 150 organizations since 2007."[177] Mandiant asserted APT1 is most likely a Chinese Army cyber unit.[178] ; although China denounced the accusations, the U.S. government shifted from oblique allusions to openly calling China out as a significant source of cyber events.[179] On one hand, Mandiant's vocal attribution of cyber meddling to China facilitated the ability of the U.S. to attribute bad acts to China.[180] On the other hand, it

---

[175] *Id.* The goal of the NIST Framework is to guide the development of a voluntary risk-based approach to cybersecurity. NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf [https://perma.cc/2FHW-E2L9].

[176] John J. Chung, *Critical Infrastructure, Cybersecurity, and Market Failure*, 96 OR. L. REV. 441, 449-50 (2018). Per the Critical Infrastructure Protection Act of 2001, critical infrastructures are the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." *Id*. at 446 (citing Critical Infrastructures Protection Act of 2001, 42 U.S.C. § 5195c(e) (2012)). Per the Department of Homeland Security, there are sixteen critical infrastructure sectors: "(1) chemical sector; (2) commercial facilities sector; (3) communications sector; (4) critical manufacturing sector; (5) dams sector; (6) defense industrial base sector; (7) emergency services sector; (8) energy sector; (9) financial services sector; (10) food and agriculture sector; (11) government facilities sector; (12) healthcare and public health sector; (13) information technology sector; (14) nuclear reactors, materials and waste sector; (15) transportation systems sector; and (16) water and wastewater systems sector." *Id*.

[177] Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 318-19 (2015).

[178] *Id*. at 319.

[179] *Id*.

[180] *Id.*

meant the government's hand may have been forced by a private entity into taking action before it was either ready or tactically sound to do so.

In many respects, the U.S. operates a de facto public-private cybersecurity system wherein the private sector shoulders a quasi-governmental role and where the federal government sometimes acts more like a market participant than a traditional regulator.[181] For instance, "private companies investigate networks of malware-infected systems used by transnational criminal groups for financial fraud," while the government has become a true market participant by buying software vulnerabilities on the gray market and purposefully not disclosing them to software makers that could remedy the flaws.[182] Yet, "[t]he private sector is struggling to contend with the growing scope, scale, and complexity of cyber" operations.[183]

As it stands, the U.S. government and the private sector are stuck at an impasse concerning cybersecurity information sharing.[184] U.S. companies argue that the federal government should take an active role in its cyber defense while the intelligence community is loath to part with its classification methods lest technical sources and methods be placed at risk.[185] A solution with increasing support is a national classified cyber information-sharing network between the federal government and the private sector.[186] In this schema, an already-existing classified network for defense contractors would be expanded to private CI companies.[187] This is not entirely far-fetched since David Sanger, the Pulitzer Prize winning journalist, remarked that the U.S. should come to grips with certain realities to remain a decisive actor in the cyber domain to include ending the reflexive attitude federal cyber defenses must extend to government networks and no further.[188] It is worth noting that public-private information sharing only works when the private sector acts on the information it receives.

"On September 7, 2017, Equifax, one of the [biggest] consumer-credit reporting agencies in the world," announced that its consumer information had

---

[181] Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 471-72 (2017).

[182] *Id*. at 471.

[183] Ariel Levite et al., *Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance*, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE (Nov. 7, 2018), https://carnegieendowment.org/2018/11/07/addressing-private-sector-cybersecurity-predicament-indispensable-role-of-insurance-pub-77622 [https://perma.cc/7AYN-TAT6].

[184] Robert Knake, *Sharing Classified Cyber Threat Information with the Private Sector*, COUNCIL ON FOREIGN REL. (May 15, 2018), https://www.cfr.org/report/sharing-classified-cyber-threat-information-private-sector [https://perma.cc/TAF9-CQCJ].

[185] *Id.*

[186] *See, e.g., id.*

[187] *Id.*

[188] DAVID SANGER, THE PERFECT WEAPON: WAR, SABOTAGE, AND FEAR IN THE CYBER AGE 304-08 (2018).

been hacked.[189] The breach had actually occurred much earlier, from May to July 2017, when "the hackers gained access to the names, Social Security numbers, birth dates, addresses and driver's license numbers of" 145.5 million U.S. consumers.[190] "The Department of Homeland Security (DHS) alerted Equifax on March 8, 2017 that it needed to remedy a critical security flaw in its software which would have prevented the hack, but company officials took no action and the infamous catastrophic breach is now history.[191]

D. Red Cyber

On November 24, 2014, the so-called "Guardians of Peace" hackers stole terabytes of data from Sony Pictures Entertainment.[192] Sony had recently produced a comedy film titled "The Interview" and the plot of the film involved the assassination of North Korea's leader, Kim Jong Un. The hackers, likely DPRK proxies, threatened to release more confidential documents unless Sony refused to show the movie.[193] Unfortunately, many theatres across the U.S. acquiesced to the hackers' demands and pulled the movie from their lineups.[194] In the wake of the ensuing controversy, the U.S. government took an unusual step and publicly blamed North Korea for the Sony hack.[195] Following a government investigation that linked the attack's code and design to previous attacks suspected of originating in North Korea, "the State Department officially condemned North Korea on December 19, 2014," and President Obama vowed in a press release the U.S. would respond proportionally in the arena of its choosing.[196]

At the time, some claimed the Sony hack was an example of "cyberwarfare" while academics and specialists clarified that the hack did not meet the legal

---

[189] McKay Smith & Garrett Mulrain, *Equi-Failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform*, 9 J. NAT'L. SEC. L. & POL'Y 549, 553 (2018).

[190] *Id*. at 553-54.

[191] *Id*. at 555.

[192] Beatrice A. Walton, *Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law*, 126 YALE L.J. 1460, 1462 (2017).

[193] Walton, *supra* note 192, at 1462. *See also* Catherine Shoard, *Sony Hack: The Plot To Kill the Interview – a Timeline So Far*, GUARDIAN (Dec. 18, 2014), http://www.theguardian.com/film/2014/dec/18/sony-hack-the-interview-timeline [https://perma.cc/5W6W-U9LG].

[194] Walton, *supra* note 192, at 1462.

[195] *Id.* at 1462-63; Ellen Nakashima, *U.S. Attributes Cyberattack on Sony to North Korea*, WASH. POST (Dec. 19, 2014), http://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html.

[196] Walton, *supra* note 192, at 1463. *See also, Remarks by the President [Barack Obama] in Year-End Press Conference*, WHITE HOUSE (Dec. 19, 2014), http://www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference [https://perma.cc/3MMK-SQLK].

requirement for that title.[197] Yet, if the Sony hack was not cyberwarfare, it was nonetheless hard to precisely define its characteristics. The hack was akin to cyberespionage and transnational cybercrime, but there were added troublesome elements.[198] For instance, distinct from most cyberespionage acts, the stolen information was intentionally aired to the public with apparent malicious intent.[199] Similarly, unlike much transnational cybercrime, the event was state-sponsored, and while in theory individual members of the "Guardians of Peace" may be held criminally responsible, North Korea cannot.[200]

In cyber operations, a use of force occurs "when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[201] According to Tallinn Manual 2.0, a cyberattack is "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[202] Yet "[t]he problem is not the lack of definitions, but a lack of consensus about what bad conduct in cyberspace really needs to be stopped."[203] In regards to what "bad conduct" in the cyber domain legitimately rises to the level of an armed attack, international legal scholar Yoram Dinstein provides multiple examples: "[f]atalities caused by the loss of computer-controlled life-support systems; an extensive power grid

[197] Crootof, *supra* note 168, at 568-69. *See generally*, Ryan Goodman, *International Law and the US Response to Russian Election Interference*, JUST SECURITY (Jan. 5, 2017), https://www.justsecurity.org/35999/international-law-response-russian-election-interference/ [https://perma.cc/E3QS-JQBK] (discussing what constitutes an act of war). *See also* Peter W. Singer & Allan Friedman, *5 Lessons from the Sony Hack*, CNN (Dec. 17, 2014), http://www.cnn.com/2014/12/17/opinion/singer-friedman-sony-hacking-lessons/index.html [http://perma.cc/6X6X-XUDR] ("The hack of Sony has often been lumped in with stories ranging from run of the mill online credit card theft to the Target, Home Depot and JP Morgan breaches to the time that Iranian-linked hackers allegedly 'erased data on three-quarters of Aramco's corporate PCs.' . . . It's a lot like lumping together every incident in New York that involves a gun, whether it's a bank robbery, a murder or a football player accidentally shooting himself.").

[198] Crootof, *supra* note 168, at 569.

[199] *Id.*

[200] *Id.*

[201] NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 330 (Michael N. Schmitt ed., 2d ed., 2017). Former State Department Legal Adviser Harold Hongju Koh laid out the U.S. position in 2012 when he said cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force. *See* Harold Hongju Koh, *International Law in Cyberspace*, 54 HARV. INT'L. L.J. ONLINE 1, 8 (Dec. 2012), http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf [https://perma.cc/DQU4-2G3C].

[202] NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, *supra* note 200, at 415.

[203] Michael Sulmeyer, *Which Cyberattacks Should the US Deter, and How Should it be Done?*, COUNCIL ON FOREIGN REL. (July 24, 2017), https://www.cfr.org/blog/which-cyberattacks-should-united-states-deter-and-how-should-it-be-done [https://perma.cc/R927-L9LZ].

outage . . . creating considerable deleterious repercussions; a shutdown of computers controlling waterworks and dams . . . generating thereby floods of inhabited areas; deadly crashes deliberately engineered."[204] Cataracts persist in this logic flow, however, because some attacks do not produce kinetic effects but instead harm data and data systems. Further, cyber confounds, in certain respects, long-standing notions of state responsibility. According to the 2018 U.S. Department of Defense National Defense Strategy Summary:

> States are the principal actors on the global stage, but *non-state actors* also threaten the security environment with increasingly sophisticated capabilities." Terrorists, trans-national criminal organizations, cyber hackers and other malicious non-state actors have transformed global affairs with increased capabilities of mass disruption.[205]

In other words, cyber operations below the use of force level exist in a twilight zone of international law.[206] In April 2018, former Department of Homeland Security Secretary Jeh Johnson testified before the House Armed Services Committee regarding questions about what cyber acts constitute an act of war and his disconcerting response was "we will know it when we see it."[207]

China was the prime suspect in the hacking of the U.S. Office of Personnel Management ("OPM") in December 2014.[208] The damage was so extensive that the U.S. opened cyber security negotiations with China.[209] In September 2015, joint statements by Chinese President Xi Jinping and President Obama declared both states would refrain from certain malicious cyber activities.[210] Soon thereafter, other countries made similar announcements.[211] Some heralded a

---

[204] Jessica Malekos Smith, *Swinging A Fist in Cyberspace*, 9 HOUS. L. REV. 1, 3-4 (2018).

[205] U.S. DEP'T OF DEFENSE, SUMMARY OF THE 2018 NATIONAL DEFENSE STRATEGY OF THE UNITED STATES OF AMERICA 3 (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf [https://perma.cc/K7M7-YMDW].

[206] *See* Harvey Rishikof et al., *Gray Zone: As State Actors Continue to Wage Cyberwar on the United States, They Have A Powerful Ally-Gaps and Ambiguities in the Law*, ABA J., Nov. 2018, at 30, 30-31 (state actors take advantage of gaps and ambiguities to commit cyber operations against the United States).

[207] *Hearing on Cyber Operations Today: Preparing for 21st Century Challenges in an Information-Enabled Society Before the H. Armed Services Comm.* (Apr. 11, 2018) (statement of Jeh Charles Johnson, former Sec'y of Homeland Security).

[208] *Id*.

[209] Christina Lam, *A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election*, 59 B.C. L. REV. 2167, 2173 (2018).

[210] *Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference*, WHITE HOUSE (Sept. 25, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint [https://perma.cc/AJ46-YD3H] (discussing the cyber agreement between the United States and China).

[211] *See, e.g.*, Thomas Escritt & Michelle Martin, *Ahead of Fractious G20, Germany and China Pledge New Cooperation*, REUTERS (July 5, 2017),

possible softening in China's stance toward cyber aggression but cyber norms, especially hortatory ones, are not enforceable by states.[212] For a period of time, it appeared the cyber agreement between China and the U.S. led to decreased cyber aggression on the part of China.[213] On October 4, 2017, former Attorney General Jeff Sessions met with his Chinese counterpart and confirmed they would continue "implementation of the consensus reached" by President Xi and President Obama in 2015.[214] Yet China was soon back to its old tricks.[215] In 2017, at President Trump's direction, U.S. Trade Representative Robert Lighthizer undertook a seven-month investigation into China's cyber theft of American intellectual property ("IP") and found "strong evidence that China uses foreign-ownership restrictions to compel American companies to switch technology to local firms and that China supports and conducts cyberattacks on U.S. companies to access trade secrets."[216] Experts believe China is responsible for between $225 to $600 billion in annual IP theft.[217] Richard Ellings, executive director of the Commission on the Theft of American Intellectual Property recently stated that China's behavior is "an assault the likes of which the world has never seen. . . . You can't find a company that hasn't been assaulted, and

https://www.reuters.com/article/us-g20-germany-china/ahead-of-fractious-g20-germany-and-china-pledge-new-cooperation-idUSKBN19Q16R [https://perma.cc/8X7H-4V3V] (describing an agreement between China and Germany); Rowena Mason, *Xi Jinping State Visit: UK and China Sign Cybersecurity Pact*, GUARDIAN (Oct. 21, 2015), https://www.theguardian.com/politics/2015/oct/21/uk-china-cybersecurity-pact-xi-jinping-david-cameron [https://perma.cc/U252-Y6HT] (showcasing a new cyber-security agreement between China and the United Kingdom).

[212] Kathleen Claussen, *Beyond Norms: Using International Economic Tools to Deter Malicious State-Sponsored Cyber Activities*, 32 TEMP. INT'L & COMP. L.J. 113, 113-14 (2018).

[213] Joseph Menn & Jim Finkle, *Chinese Economic Cyber-Espionage Plummets in U.S.: Experts*, REUTERS (June 21, 2016) http://www.reuters.com/article/us-cyber-spying-china-idUSKCN0Z700D [https://perma.cc/22VA-NESZ].

[214] Press Release, Dep't of Justice Office of Pub. Affairs, First U.S.-China Law Enforcement and Cybersecurity Dialogue (Oct. 6, 2017), https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue [https://perma.cc/5KRJ-E5TT].

[215] Ken Dilanian, *China's Hackers Are Stealing Secrets from U.S. Firms Again, Experts Say*, NBC NEWS (Oct 9, 2018), https://www.nbcnews.com/news/china/china-s-hackers-are-stealing-secrets-u-s-firms-again-n917836 [https://perma.cc/RC2S-WARB] (explaining how China increased its thefts of U.S. trade secrets following a lull in the last year of the Obama Administration).

[216] Grant Clark, *What Is Intellectual Property, and Does China Steal It?,* BLOOMBERG (Dec. 4 2018), https://www.bloomberg.com/news/articles/2018-12-05/what-s-intellectual-property-and-does-china-steal-it-quicktake [https://perma.cc/V723-CKWF].

[217] Sherisse Pham, *How Much Has the US Lost From China's Theft*?, CNN: MONEY (Mar. 23, 2018), https://money.cnn.com/2018/03/23/technology/china-us-trump-tariffs-ip-theft/index.html [https://perma.cc/A3EK-68PV].

half of them don't even know it."[218] In retaliation President Trump hit China with tariffs on $200 billion worth of Chinese goods.[219] However, instead of the tariffs acting as a deterrent and punishing China for its actions, reports indicate China stepped up hacking operations against the U.S.[220] As a result, the Trump Administration is beginning to move beyond a tariff-only approach and is broadening its trade battle with China using a plan to use export controls and indictments to deter China's cyber aggression.[221]

China is unquestionably a first-rate cyber power.[222] In February 2014, the Chinese Communist Party created the "Cybersecurity and Informatization Leading Group," chaired by President Xi Jinping, to address cybersecurity concerns.[223] The establishment of the group showcases how senior leaders in China view cyber as a critical national priority.[224] In June 2017, China ushered in a hardline cyber law requiring domestic and foreign firms to submit to security checks and store user data within the country.[225] According to the U.S. perspective, China's new cyber law "would disrupt, deter, and in many cases, prohibit cross-border transfers of information that are routine in the ordinary course of business."[226] At the same time, China continues to hack the Department of Defense ("DoD") and DoD contractors.[227] Indeed, "Beijing has been very good at . . . targeting U.S. defense contractors, getting into their computer systems through various types of essentially cyber warfare and

[218] Michael Collins, *Why Trump Tariffs on China not Stopping Theft of Trade Secrets*, USA TODAY (Nov. 28, 2018), https://www.usatoday.com/story/news/politics/2018/11/28/trade-war-china-donald-trump-theft-intellectual-property-trade-secrets/2124428002/ [https://perma.cc/SE99-SKBQ].

[219] *Id.*

[220] *Id*. In October 2018, cyber experts at the U.S. Naval War College and Tel Aviv University published a joint study detailing how China Telecom, one of China's largest telecom enterprises operating within North America hijacks internet communications in the U.S. and Canada and "diverts it to China where it is copied." *Id*.

[221] Kate O'Keefe, *U.S. Adopts New Battle Plan to Fight China's Theft of Trade Secrets*, WALL ST. J. (Nov. 12, 2018), https://www.wsj.com/articles/u-s-deploys-new-tactics-to-curb-chinas-intellectual-property-theft-1542027624 [https://perma.cc/S3TZ-2X32].

[222] Jyh-An Lee, *Hacking into China's Cybersecurity Law*, 53 WAKE FOREST L. REV. 57, 58-59 (2018).

[223] *Id.* at 64.

[224] *Id.* at 64-65.

[225] Tom Miles, *U.S. Asks China not to Enforce Cyber Security Law*, REUTERS (Sept. 26, 2017), https://www.reuters.com/article/us-usa-china-cyber-trade/u-s-asks-china-not-to-enforce-cyber-security-law-idUSKCN1C11D1 [https://perma.cc/4DMS-N5U7].

[226] *Id.*

[227] *See, e.g.,* Jeff Daniels, *Chinese Theft of Sensitive U.S. Military Technology Is still a 'Huge Problem,' Says Defense Analyst*, CNBC (Nov. 8, 2017), https://www.cnbc.com/2017/11/08/chinese-theft-of-sensitive-us-military-technology-still-huge-problem.html [https://perma.cc/U2WV-E8F6].

stealing the designs of some of America's best military assets."[228] On December 20, 2018 Deputy Attorney Rod Rosenstein announced charges against Chinese hackers who allegedly compromised Managed Service Providers ("MSPs"), which "are firms that other companies trust to store, process, and protect commercial data, including [sensitive IP]."[229] Benjamin Read, senior manager for cyberespionage at FireEye, stated "MSPs are incredibly valuable targets. They are people that you pay to have privileged access to your network."[230] The indictment alleges the defendants worked for an elite hacker group known as "advanced persistent threat 10" (APT-10), in association with the Chinese military intelligence service.[231] The indictment demonstrates China's ruthless efficiency and determination in the cyber domain: "More than 90 percent of the Department's cases alleging economic espionage over the past seven years involve China. More than two-thirds of the Department's cases involving thefts of trade secrets are connected to China."[232] Summing up the situation, FBI director Christopher Wray stated: "No country poses a broader, more severe long-term threat to our nation's economy and cyber infrastructure than China. China's goal, simply put, is to replace the U.S. as the world's leading superpower, and they're using illegal methods to get there."[233]

E. From Russia @ Love

Russia is particularly adept at exploiting the "grey zones" in the international law of cyberspace.[234] From 2015 to 2016, Russian-affiliated hackers broke into

---

[228] Miles, *supra* note 225.

[229] *Deputy Attorney General Rod J. Rosenstein Announces Charges Against Chines Hackers*, U.S. DEP'T OF JUSTICE (Dec. 20, 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-announces-charges-against-chinese-hackers [https://perma.cc/Z9ZK-8WKR]. This is not the first such instance as the Justice Department brought charge against five Chinese military hackers in 2014. *See, e.g.*, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, U.S. DEP'T OF JUSTICE (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor [https://perma.cc/A9AC-3B9A].

[230] Brian Barrett, *How China's Elite Hackers Stole the World's Most Valuable Secrets* (Dec. 20, 2018), WIRED https://www.wired.com/story/doj-indictment-chinese-hackers-apt10/ [https://perma.cc/XK8J-H8PW].

[231] Press Release, Dep't of Justice Office of Pub. Affairs, *supra* note 214.

[232] *Id.*

[233] Barrett, *supra* note 230.

[234] Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. INT'L L. ONLINE 1, 1–2 (2017). The Kremlin uses military, technological, diplomatic, economic, cultural, and criminal tools to wage information warfare. Molly McKew, *Putin's Real Long Game*, POLITICO (Jan. 1, 2017), https://www.politico.com/magazine/story/2017/01/putins-real-long-game-214589 [https://perma.cc/S5S3-NEMM]. (explaining that information warfare is "not about creating an alternate truth, but eroding our basic ability to distinguish truth at all" and further that

servers of the U.S. Democratic National Committee ("DNC").[235] The subsequent release of confidential information hampered "Democrats in Congressional races, led to the resignation of the DNC Chairperson, created [difficulties] between the Clinton and Sanders camp[aigns], and figured prominently in the [presidential race]."[236] In doing so, Russia took advantage of international law principles and rules that are either "poorly demarcated" or subject to multiple interpretations.[237] For example, at issue in the DNC hacks was whether Russia's involvement was a breach of U.S. sovereignty or an instance of prohibited intervention;[238] further, if the attacks could be attributed to Russia, how should the U.S. respond proportionally and in what vein?[239]

Recall the U.S. never claimed the Sony or DNC hacks were violations of international law.[240] In regards to the Sony hack, then-President Obama opined the event was an instance of "cyber vandalism."[241] These perambulations of lexicon are perhaps evidence states are unmoored to current realities and are casting about for new ways to properly characterize a new era of cyber events "without explicitly labeling them as unlawful" and thereby creating precedent that might limit their own projected cyber end-states.[242] In other words, although the Sony and DNC events might be "world-altering," there is no term in the current language of international law to accurately describe those cyber

President Vladimir Putin's ultimate goal is not aimed at building a new pro-Russian bloc but rather an unstable world order of "all against all.").

[235] OFF. OF THE DIR. OF NAT'L INTELLIGENCE, *ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS* 2 (Jan. 6, 2017), https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf [https://perma.cc/VXP7-ZRJK].

[236] Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. INT'L L. ONLINE 1, 1 (2017); Eric Lipton, David E. Sanger & Scott Shane, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?r=0.

[237] Schmitt, *supra* note 236, at 1.

[238] *Id.* at 2. Recently, some U.S. officials questioned if sovereignty is a rule of international law such that it may be breached. Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AJIL Unbound 207, 207 (2017). This perspective is known as the "sovereignty as principle, but not rule" approach. Schmitt, *supra* note 236, at 5. *See also*
Michael N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 CHI. J. INT'L L. 30, 39-40 (2018).

[239] Sean Watts & Theodore Richard, *Baseline Territorial Sovereignty and Cyberspace*, 22 LEWIS & CLARK L. REV. 771, 831 (2018).

[240] Crootof, *supra* note 168, at 570.

[241] Brian Fung, *Obama called the Sony hack an act of "cyber vandalism." He's right.*, WASH. POST (Dec. 22, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/22/obama-called-the-sony-hack-an-act-of-cyber-vandalism-hes-right/ [https://perma.cc/687N-UKN6].

[242] Crootof, *supra* note 168, at 570.

events.[243] Accordingly, states that fall victim to aggressive and invasive cyber operations have few non-escalatory options and "the harms associated with these incidents tend to lie where they fall."[244]

NATO cybersecurity experts determined a nation-state launched the June 2017 malware hack dubbed "NotPetya."[245] Its purpose was to showcase the perpetrator's capacity to inflict damage and was essentially a "declaration of power"; a demonstration of "acquired disruptive capacity and readiness to use it."[246] NotPetya masqueraded as a ransomware event and was first aimed at disrupting Ukrainian computer systems before spreading to computers in Denmark, India, and the U.S.[247] The hackers broke into a popular Ukrainian software developer and infected its servers with destructive malware.[248] For weeks post-breach, whenever users attempted "to update their software, they would also download hidden malware."[249] Once the hackers uploaded the malware onto host systems, the software remained dormant until June 27, 2017 "when millions of hidden logic bombs went off [and caused] a rapid outbreak of the NotPetya software".[250] Ultimately, NotPetya infected businesses in more than 20 countries and caused an estimated $1.2 billion in damages.[251]

The U.S. was blunt in its assignation of blame and unequivocally held the Russian military cyber operators were behind the attack.[252] The U.S. along with the United Kingdom, argued that NotPetya was consistent with Russia's brand

---

[243] Fung, *supra* note 241.

[244] *Id.* at 571.

[245] Paul Merrion, *NATO experts say nation-state hackers likely behind NotPetya cyberattack*, CQ ROLL CALL, June 30, 2017, 2017 WL 2819920.

[246] *Id.*

[247] James E. Scheuermann, *Cyber Risks, Systemic Risks, and Cyber Insurance*, 122 PENN ST. L. REV. 613, 635 n.52 (2018); Jeremy Kirk, *Latest Ransomware Wave Never Intended to Make Money*, BANK INFO SECURITY (June 29, 2017), https://www.bankinfosecurity.com/latest-ransomware-wave-never-intended-to-make-money-a-10069 [https://perma.cc/F76E-2T3P]; Sarah Marsh, *U.S. Joins UK in Blaming Russia for NotPetya Cyber-attack*, GUARDIAN (Feb. 15, 2018), https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine [https://perma.cc/59S8-8ZRT]; Ellen Nakashima, *Russian Military was Behind 'NotPetya' Cyber Attack in Ukraine, CIA Concludes*, WASH. POST (Jan. 12, 2018), https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?utm_term=.aa4824497af1 [https://perma.cc/V5ZV-8Q6A].

[248] Henry Kenyon, *Ukraine prepares for major cyberattack with possible global implications*, CQ ROLL CALL, Oct. 18, 2017, 2017 WL 4675556.

[249] *Id.*

[250] *Id.*

[251] Andrea M. Matwyshyn, *Cyber Harder*, 24 B.U. J. SCI. & TECH. L. 450, 450 (2018).

[252] Bruce Zagaris, *U.S. Imposes Sanctions re Russian Cyber Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks*, 34 INT'L ENFORCEMENT L. REP. 112, 112 (2018).

of "hybrid warfare" aimed at destabilizing Ukraine.[253] Speaking at the annual Munich Security Conference in February 2018, Rob Joyce, the White House cybersecurity coordinator and special assistant to President Trump, said regarding NotPetya: "We're going to work on the international stage to impose consequences. Russia has to understand that they have to behave responsibly on the international stage."[254] On March 15, 2018, OFAC "designated five entities and 19 persons under the Countering America's Adversaries Through Sanctions Act (CAATSA) as well as Executive Order (E.O. 13694)"[255] Treasury Secretary Steven Mnuchin asserted "[t]he Administration is confronting and countering malign Russian cyber activity, including their attempted interference in U.S. elections . . . to conducting destructive cyber-attacks, including the NotPetya attack."[256]

NotPetya was the most destructive and costly cyber-attack in history because it "quickly spread worldwide causing billions of dollars in damage across Europe, Asia, and the Americas."[257] NotPetya had a particularly devastating impact on U.S. companies.[258] FedEx reported an estimated $300 million loss or a $79 cent loss per share in the aftermath of the event.[259] Rob Carter, FedEx's chief information officer, explained the hack "was the result of [a] nation state targeting Ukraine and companies that do business there."[260] As a result, FedEx

[253] Matwyshyn, *supra* note 251, at 451.

[254] Cristina Maza, *Russia Must Pay for NotPetya Cyberattack, Trump Cybersecurity Official Warns*, NEWSWEEK (Feb. 16, 2018), https://www.newsweek.com/russia-must-pay-its-notpetya-cyber-attack-trump-cybersecurity-official-warns-809880 [https://perma.cc/M3HX-WX5K].

[255] Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks (Mar. 15, 2018), https://home.treasury.gov/news/press-releases/sm0312 [https://perma.cc/XJ6K-HSYP].

[256] *Id.*

[257] WHITE HOUSE, Statement from the Press Secretary (Feb. 15, 2018), https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/ [https://perma.cc/DQX2-UH9Q]; Similar to WannaCry, NotPetya entailed cascading adverse effects of cyber events; it masqueraded as cyber extortion but had alternate motives. James E. Scheuermann, *Cyber Risks, Systemic Risks, and Cyber Insurance*, 122 PENN ST. L. REV. 613, 635 (2018).

[258] *See, e.g.,* Lee Mathews, *NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million*, FORBES (Aug. 16, 2017), https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#603c1f934f9a [https://perma.cc/K3X2-JKHF].

[259] Zaid Shoorbajee, *FedEx attributes $300 million loss to NotPetya Ransomware Attack*, CYBERSCOOP (Sept. 20, 2017), https://www.cyberscoop.com/fedex-attributes-300-million-loss-notpetya-attack/ [https://perma.cc/3MWG-NQLK].

[260] John Leyden, *FedEx: TNT NotPetya Infection Blew a $300 million Hole in Our Numbers*, REGISTER (Sept. 20, 2017), https://www.theregister.co.uk/2017/09/20/fedex_notpetya_damages/ [https://perma.cc/DY42-SHUB].

chose to invest in cyber protection and resiliency technology.[261] Merck, the global pharmaceutical giant with its headquarters in New Jersey, reported NotPetya "disrupted manufacturing, research and sales operations [which left it] unable to fulfill orders for certain essential products [like] the Gardasil 9 vaccine, which prevents cancers and other diseases caused by the human papillomavirus."[262] NotPetya cost Merck almost $670 million in damages in 2017.[263] The complete disruption led Congress to request a formal briefing with Merck's CEO.[264] In a letter from the House Committee on Energy and Commerce, Congress expressed NotPetya "raise[d] questions about how the nation is prepared to address a significant disruption to critical medical supplies" as a result of a cyber event.[265]

NotPetya was both crafty and quick and in certain instances it infected one thousand computers in less than two minutes.[266] According to Alan Brill, senior managing director at the cyber risk firm Kroll Inc., "NotPetya was really there to cause irreparable damage and make . . . data permanently unavailable. . . . Anybody who thinks this kind of thing couldn't happen again is naïve."[267] NotPetya "was a wake-up call to companies and their executives [and it highlighted] how unprepared . . . systems were to face [sophisticated] attacks and the time and money it would take" for companies, in particular corporations with global enterprises, to recover.[268] According to Andrea Matwyshyn, professor of law and computer science at Northeastern University, NotPetya raises the specter companies will increasingly be drawn into transnational conflicts because "[i]f you want to damage the U.S., one way to do that is to

[261] *See* Samantha Ann Schartz, *After NotPetya, FedEx Invests In Security And Flexible IT*, CIO DIVE (June 26, 2018), https://www.ciodive.com/news/after-notpetya-fedex-invests-in-security-and-flexible-it/526534/ [https://perma.cc/NN3P-9JFL].

[262] *See* MERCK COMPANY FACT SHEET, https://www.merck.com/about/our-history/facts/home.html [https://perma.cc/6YBH-B3DZ]; Kim Nash, *One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs*, WALL ST. J. (June 27, 2018), https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906 [https://perma.cc/442B-PFJG].

[263] Nash, *supra* note 262.

[264] Letter from Greg Walden, Chairman, House of Representatives Comm. on Energy & Com. & Tim Murphy, Chairman, Subcomm. On Oversight & Investigations, to Kenneth Frazier, Chairman & Chief. Exec. Officer, Merck & Co., Inc. (Sept. 20, 2017) [hereinafter Comm. On Energy & Com. Letter to Merck], *as quoted in* Brandi Buchman, *Congress Asks Merck for Information on Cyberattack*, COURTHOUSE NEWS SER. (Sept. 21, 2017), https://www.courthousenews.com/congress-asks-merck-information-cyberattack/ [https://perma.cc/URU5-M5Y8].

[265] Buchman, *supra* note 264.

[266] Nash, *supra* note 262.

[267] *Id.*

[268] *Id.*

damage its biggest companies."[269] In a short statement just under either months after the attack, the White House blamed Russia for the event, stating:

> "NotPetya," quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. It was part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences.[270]

The media covering NotPetya asserted the U.S. was finally taking a stand against Russian cyber aggression; a typical headline from CNN read "White House Blasts Russia for NotPetya Cyberattack."[271] Speaking of Russia's involvement, Tonya Ugoretz, director of the Cyber Threat Intelligence Integration Center in the Office of the Director of National Intelligence said Russian "aggression is widespread. It's against multiple sectors. It's against multiple types of networks. . . . It wasn't just aimed at the government. It was really aimed at all of us."[272] Within a few days after the U.S. blamed Russia for NotPetya, six other nations — the United Kingdom, Australia, Canada, Denmark, Lithuania, and Estonia — called out Russia in official statements.[273] Australia's Ambassador for Cyber Affairs noted the group attribution was no coincidence but rather:

> What we're doing is maturing [cyber attribution] in order that the consequences will be felt further in the future. [A] key part of deterrence is signaling to another country, to provide clear, consistent, and credible messaging to adversaries that there will be repercussions for the behavior that they're conducting.[274]

---

[269] *Id.*

[270] Statement from the Press Secretary, *supra* note 257.

[271] Sophie Tatum, *White House blasts Russia for NotPetya Cyberattack*, CNN (Feb. 15, 2018), https://www.cnn.com/2018/02/15/politics/white-house-russia-notpetya/index.html [https://perma.cc/7D88-NG5X]. *See also* Aaron Mak, *The U.S. Says It Will Strike Back at Russia for the NotPetya Cyberattack*, SLATE (Feb. 16, 2018), https://slate.com/technology/2018/02/after-officially-blaming-russia-for-the-notpetya-virus-u-s-officials-promise-consequences.html [https://perma.cc/6GAJ-M3YT] ("White House Press Secretary Sarah Huckabee Sanders had also hinted at retaliation in a statement . . . which was uncharacteristically forceful given the administration's usual sheepishness in calling out the Kremlin.").

[272] *Transcript: The Cyber 202 Live*, WASH. POST (July 20, 2018), https://www.washingtonpost.com/blogs/post-live/wp/2018/07/20/transcript-the-cyber-202-live/?noredirect=on&utm_term=.73ae5e51792d [https://perma.cc/SZ24-CBVU].

[273] Stil Gherrian, *Blaming Russia for NotPetya was Coordinated Diplomatic Action*, ZDNET (Apr. 12, 2018), https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/ [https://perma.cc/P87P-F3TH].

[274] *Id.*

More recently, in October 2018, the Justice Department "charged seven Russian intelligence [agents] with hacking doping agencies and other organizations such as a Pennsylvania-based nuclear energy company."[275] John Demers, assistant attorney general for the Justice Department's National Security Division, detailed the indictment which:

> alleges Russia's military intelligence agency, the known as the GRU, targeted . . . victims because they had publicly [castigated] Russia's state-sponsored athlete doping program. . . . The seven intelligence officers were all charged with computer hacking, wire fraud, aggravated identity theft and money laundering.[276]

Yet, because the private sector has a paucity of options during ongoing breaches due to government inattention and lack of willingness to become involved, their options appear like a series of Hobbesian choices: shed operations in areas of turmoil like Ukraine; enter the emerging and volatile market of cyber insurance;[277] protect oneself through the use of hack-backs while likely violating the law[278]; or endure the numbing reality of a state of eternal breach.

V. A STRATEGY FOR VICTORY

A. New Tactics, Old Adversaries

On the morning of February 5, 2016[279], Zubair Bin Huda, a director at Bangladesh's Central Bank, entered its headquarters building in Dhaka and

---

[275] Kevin Breuniger, *Russian Department Charges 7 Russian Hackers with Targeting Doping Agencies, Nuclear Energy Company*, CNBC (Oct. 4, 2018), https://www.cnbc.com/2018/10/04/doj-charges-7-russian-intelligence-operatives-with-hacking.html [https://perma.cc/TT8P-6LHS].

[276] *Id.* The concept of deterrence is an old one in the history of national security. Zachary K. Goldman & Damon McCoy, *Deterring Financially Motivated Cybercrime*, 8 J. NAT'L. SEC. L. & POL'Y 595, 595 (2016). Despite the pedigree of deterrence as a strategy, the cyber domain in meaningful measure has failed to apply it to cybersecurity and cybercrime. *Id.* Former NSA Director Admiral Michael Rogers recently declared, regarding cyberspace, "the 'fundamental concepts of deterrence [are] immature.'" *Id.* Cyber deterrence has foundered, in part, due to the unique challenges inherent in the cyber domain including the difficulty of attributing cyber events to particular actors and the reticence of states to discuss capabilities they regard as highly classified. *Id.*

[277] *See* Kevin DiGrazia, *Cyber Insurance, Data Security, and Blockchain in the Wake of the Equifax Breach*, 13 J. BUS. & TECH. L. 255, 260 (2018) (stating that cyber insurance is "a relatively new product" and "is a virtual wild west of insurance policies with no standardization of coverage or policy language, which makes it [difficult] to compare policy pricing and coverage.").

[278] *See* discussion *infra* Section V.

[279] Priyanka Boghani, *The U.S. and North Korea On the Brink: A Timeline*, FRONTLINE (Apr. 18, 2018), https://www.pbs.org/wgbh/frontline/article/the-u-s-and-north-korea-on-the-brink-a-timeline/ [https://perma.cc/MMZ4-UNZQ]. In October 2006, North Korea conducted its first nuclear test with an "explosion yield[ing] less than a kiloton . . . the atomic bomb that

made a disconcerting discovery.[280] The bank was previously stuck in the analog age but with a new bank governor at the helm, the institution took the digital plunge in 2009.[281] By 2016 the bank used the SWIFT (Society for Worldwide Interbank Financial Telecommunication) transmission process, the gold standard in electronic banking wherein money moves through the dispatching of encrypted messages to multiple operating centers and onward to receivers.[282] As duty manager, Bin Huda was charged with reviewing SWIFT transactions for possible errors or mistakes.[283] This morning his eyes fell upon a disquieting message: "A file is missing or changed."[284] The error message meant Bin Huda was in the middle of the world's largest and boldest bank robbery.[285]

To accomplish the heist, hackers sent thirty-five SWIFT orders signaling transfer of $951 million out of the bank's account at the Federal Reserve Bank of New York ("Federal Reserve") to multiple private accounts around the world.[286] Ultimately, the Federal Reserve was duped into paying out $101 million.[287] The losses may have been graver save but for a single lightning bolt of good fortune — the name "Jupiter" formed part of a Philippines bank address where the robbers sought to send money, but "Jupiter" was likewise the name of a prohibited shipping company due to the U.S. sanctions regime against Iran.[288] The Federal Reserve zeroed in on the suspicious transfer and examined the

destroyed Hiroshima was fifteen kilotons." *Id*. In 2009, North Korea tested a second nuclear device estimated at four kilotons. *Id.* From 2012 to 2016, North Korean nuclear testing accelerated as well as achieved technological advances in ballistic missile technology. *Id.*

[280] Joshua Hammer, *The Billion-Dollar Bank Job*, N. Y. TIMES (May 3, 2018), https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html [https://perma.cc/8VZT-NPQA]. Serious bank robbers no longer make a living with a ski mask and pistol. Julie Andersen Hill, *Swift Bank Heists and Article 4a*, 22 J. CONSUMER & COM. L. 25, 25 (2018). Current bank security protocols mean typical heists garner only $6,500 and half the perpetrators are caught. *Id.*

[281] Hammer, *supra* note 280.

[282] *Id.*

[283] *Id.*

[284] *Id.*

[285] *Id.*; Criminal Complaint at 1-3, U.S. v. Park Jin Hyok (C.D. Cal. 2018) (No. MJ18-1479). It was foreseeable that the hackers likely breached the bank's network, as it lacked sufficient firewall protection. Kim Zetter, *That Insane, $81M Bangladesh Bank Heist? Here's What We Know*, WIRED (May 17, 2016) https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/ [https://perma.cc/DG2H-943N].

[286] Jamie Schram, *Congresswoman wants probe of 'brazen' $81M theft from New York Fed*, NEW YORK POST (Mar. 22, 2016), https://nypost.com/2016/03/22/congresswoman-wants-probe-of-brazen-81m-theft-from-new-york-fed/ [https://perma.cc/52WB-N4RG].

[287] *Id*.

[288] Krishna Das and Jonathan Spicer, *The SWIFT Hack: How the New York Fed fumbled over the Bangladesh Bank cyber-heist*, REUTERS (Oct. 2, 2018), https://web.archive.org/web/20181002135750/https://www.reuters.com/investigates/special-report/cyber-heist-federal/ [https://perma.cc/F7RJ-AKXG].

fraudulent orders more closely.[289] In addition to the fated name similarity, the payment orders contained format flaws and, inconsistent with usual practice, were addressed mainly to individuals.[290] Nonetheless, despite the Federal Reserve's best efforts, by the time the warning signs were recognized and actioned, it approved five payments and sent $101 million from Bangladesh Bank funds winging their way to accounts in Sri Lanka and the Philippines including a surprising $81 million to four accounts in the name of individual persons.[291] The vast majority of the funds were never recovered.[292]

A full year after the brazen digital hold-up, U.S. prosecutors built the case and found that North Korean hackers, aided by Chinese cyber experts, were responsible for the robbery.[293] On March 21, 2017, former National Security Agency (NSA) Deputy Director Rick Ledgett said that if North Korea was behind the heist, it meant the rogue regime was employing game-changing tactics and was "'a big deal.'"[294] In Ledgett's view, the bank robbery marked a dangerous escalation for North Korea and showcased Pyongyang[295] is a capable, daring, and dangerous cyberspace foe.[296]

On June 8, 2018, the U.S. charged North Korean programmer Park Jin Hyok with conspiracy and conspiracy to commit wire fraud regarding the Sony Pictures hack, the WannaCry ransomware event, and the Bangladesh Central Bank robbery.[297] The affidavit portion of the criminal complaint against Park states the Bangladesh Bank robbery was:

---

[289] *Id.*

[290] *Id.*

[291] *Id.*

[292] *Id.*

[293] *See generally* Criminal Complaint, *supra* note 285.

[294] Elias Groll, *NSA Official Suggests North Korea Was Culprit in Bangladesh Bank Heist*, FOREIGN POLICY (Mar. 21, 2017), https://foreignpolicy.com/2017/03/21/nsa-official-suggests-north-korea-was-culprit-in-bangladesh-bank-heist/ [https://perma.cc/76M5-F6ZZ]. *See also* Jim Finkle, *Cybersecurity Firm: More Evidence North Korea Linked to Bangladesh Heist,* REUTERS (Apr. 3, 2017), https://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea/cyber-security-firm-more-evidence-north-korea-linked-to-bangladesh-heist-idUSKBN1752I4 [https://perma.cc/3DPD-L68C].

[295] Criminal Complaint, *supra* note 285, at 3-4.

[296] Groll, *supra* note 294.

[297] Criminal Complaint, *supra* note 285 at 3-4. In May 2017, a malicious software, WannaCry, breached cyber systems in dozens of nations. Among its effects, the operation shut down patient files access in Britain's National Health Service and many of its hospitals. Nicole Perlroth & David E. Sanger, *Hackers Use Tool Taken From N.S.A. in Global Attack*, N.Y. TIMES (May 13, 2017), https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html [https://perma.cc/P7L5-GVFX]; *see also* Russell Goldman, *Ransomware: How Hackers Hold Data Hostage*, N.Y. TIMES (May 13, 2017), https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html [https://perma.cc/X5HP-YVVL]. Ransomware attacks, a category of malicious software that threatens to publish the host's data or block access to it until a ransom

> [T]he largest . . . cyber-theft from a financial institution to date—and [North Korean hackers] engaged in computer intrusions and cyber-heists at many more financial services victims in the United States, and in other countries in Europe, Asia, Africa, North American, and South American in 2015, 2016, 2017, and 2018, with attempted losses well over $1 billion.[298]

The Treasury Department said Park acted as an agent of the North Korean regime and announced financial sanctions against Park and the government-controlled company Chosun Expo Joint Venture, asserting that:

> North Korea . . . demonstrated a pattern of disruptive and harmful cyber activity that is inconsistent with the growing consensus on what constitutes responsible state behavior in cyberspace. . . . Our policy is to hold North Korea accountable and demonstrate . . . there is a cost to its provocative and irresponsible actions.[299]

Unfortunately, because the U.S. has no formal diplomatic relations with North Korea, Park and his fellow conspirators are unlikely to face justice in an American courtroom.[300]

B. Predictive Analysis

In a recent press conference, National Security Adviser John Bolton said that Iran has been "the world's central banker of international terrorism since 1979."[301] The complexity of U.S.-Iran relations starting from 1980 is summarized below:

---

is paid, are common but the WannaCry attack received widespread attention because its victims were global, high profile, and sophisticated. *Id*.

[298] Criminal Complaint, *supra* note 285, at 3-4.

[299] Zack Whittaker, *US Treasury Sanctions North Korea Over Sony Hack and WannaCry Attack*, TECHCRUNCH (Sept. 6, 2018), https://techcrunch.com/2018/09/06/us-treasury-sanctions-north-korean-hackers-over-sony-hack-wannacry-attack/ [https://perma.cc/XP2P-YHT9]. North Korea has stolen approximately $650 million by hacking more than one hundred banks and cryptocurrency exchanges around the globe. Patrick Winn, *How North Korean Hackers Became the World's Greatest Bank Robbers*, PRI (May 16, 2018), https://gpinvestigations.pri.org/how-north-korean-hackers-became-the-worlds-greatest-bank-robbers-492a323732a6 [https://perma.cc/7FVJ-FP8H].

[300] *U.S. Charges North Korean Over Bangladesh Bank Hack*, FINEXTRA (Sept. 6, 2018), https://www.finextra.com/newsarticle/32623/us-charges-north-korean-over-bangladesh-bank-hack [https://perma.cc/TH46-VR3R].

[301] Rebecca Morin, *White House Targets Iran with New Counterterrorism Strategy*, POLITICO (Oct. 4, 2018, 4:46 PM), https://www.politico.com/story/2018/10/04/white-house-iran-strategy-869511 [https://perma.cc/CX7G-T9LM]. *See also* Adam Shaw, *Pompeo, at Site of Obama's Address to Muslim World, Rebukes his Legacy: 'Age of Self-Inflicted American Shame is Over*', FOX NEWS (Jan. 10, 2019), https://www.foxnews.com/politics/pompeo-at-site-of-obamas-address-to-muslim-world-rebukes-his-legacy-age-of-self-inflicted-american-shame-is-over [https://perma.cc/3QWX-Q2Q4] (stating that the U.S.' "desire for peace at any cost led us to strike a deal with Iran").

> The United States and Iran have not had direct diplomatic relations since 1980. In 1979, Iranian revolutionaries held more than fifty American diplomats and citizens hostage for 444 days. During the hostage crisis, the U.S. imposed the first of many sanctions regimes on Iran, freezing all Iranian assets until 1981, when the hostages were released. The Reagan administration reinstated trade restrictions in response to Iran's state sponsorship of terrorism . . . prohibiting nearly all imports from Iran to the United States.
>
> Iran continued to sponsor terrorism in the region into the 1990s, including Hamas militants opposed to the Middle East peace process. When Iran then revived its efforts to enrich uranium, President Clinton . . . imposed a full trade and investment embargo, barring all U.S. trade with Iran. Congress went a step further and passed the Iran and Libya Sanctions Act of 1996 (now known as the Iran Sanctions Act, or ISA) which . . . imposed U.S. trade penalties on foreign companies determined to have invested more than $20 million in Iranian petroleum development. . . .
>
> However, the Clinton and then Bush administrations preferred to use diplomatic pressure to convince foreign companies to leave the Iranian market rather than impose sanctions using the ISA authorities. . . .
>
> By 2006, Iran's progress toward a nuclear weapon reached a crisis point [and] the global community responded from 2006 to 2010 with new United Nations (UN) sanctions . . . in a series of UN Security Council Resolutions (UNSCRs). Critically, UNSCR 1929 in 2010 recognized a "potential connection between Iran's revenues derived from its energy sector and the funding of Iran's proliferation-sensitive nuclear activities."[302] Claiming international legitimacy from the UNSCR language, the United States revived the ISA secondary sanctions regime and expanded it with new legislation aimed at cutting off all foreign support to Iran's energy sector.[303]

In 2015, the Obama Administration, alongside the P5+1 Group — comprised of the U.S., United Kingdom, France, China, Russia and Germany — agreed to a long-term deal with Iran regarding its nuclear program.[304] Per the accord, "Iran agreed to limit its sensitive nuclear activities and allow in international inspectors in return for the lifting of crippling economic sanctions."[305] The agreement was termed the Joint Comprehensive Plan of Action ("JCPOA") and

---

[302] *Id.* at 247.

[303] S. Riane Harper, *Can U.S. Sanctions on Iran Survive Iran's World Trade Organization Accession*?, 73 N.Y.U. ANN. SURV. AM. L. 243, 245-47. *See also* Morin, *supra* note 301.

[304] *Iran Nuclear Deal: Key Details*, BBC NEWS (May 8, 2018), https://www.bbc.com/news/world-middle-east-33521655 [https://perma.cc/5XFB-SFKN].

[305] *Id.*

was a signature foreign policy achievement for President Obama.[306] At the time, the Republican-controlled Congress was skeptical about JCPOA because it perceived Iran as untrustworthy and was sympathetic to Israel's security concerns over the deal.[307] On May 8, 2018, the Trump Administration ended U.S. participation in JCPOA.[308] President Trump declared JCPOA was "so poorly negotiated that even if Iran fully complies, the regime can still be on the verge of a nuclear breakout in just a short period of time."[309]

An analysis of Iran's behavior post-Stuxnet through the end of the JCPOA is highly valuable because it offers a blueprint for how cyber defenders can and should view the world.[310] From this analysis, it is clear that reliable predictive analysis that informs defensive postures and protocols is the single most valuable commodity for cyber defenders and ultimately sovereign nations:

> Starting in 2009, Iran's uranium centrifuges began failing, and nobody understood why. Nearly one thousand of Iran's six thousand centrifuges were destroyed over the course of a year. In the summer of 2010, a computer security firm in Belarus was hired to troubleshoot Iranian computers that mysteriously kept crashing—and in this investigation, the firm stumbled upon a series of files that would later become known as the Stuxnet virus. The Stuxnet virus was recognized as the "world's first digital weapon." It was a complex malware designed to infiltrate secure Iranian nuclear facilities, infect the industrial controllers that operated the nuclear centrifuges, and destroy those centrifuges by manipulating the pressure levels and rotor speeds inside them . . . [d]espite the significant attempt to cover its origins, experts concluded that Stuxnet was a joint United States and Israeli production.[311]

On the eleventh anniversary of 9/11, an Iranian group calling itself the "Cyber Fighters of IZZ ad-Din al-Qassam" claimed credit for a series of targeted operations against specific U.S. financial institutions.[312] The distributed denial of service (DDoS) attacks against the New York financial sector were conducted

---

[306] David E. Bernstein, *Constitutional Hardball Yes, Asymmetric Not So Much*, 118 COLUM. L. REV. ONLINE 207, 223 (2018).

[307] *Id.* at 224.

[308] *Remarks by President Trump on the Joint Comprehensive Plan of Action*, WHITE HOUSE (May 8, 2018, 2:13 PM), https://www.whitehouse.gov/briefings-statements/remarks-president-trump-joint-comprehensive-plan-action/ [https://perma.cc/LU2B-CYNJ].

[309] *Id.*

[310] *See* Nicole Pasulka, *A Virus Altered the Face of Security in Iran*, TAKEPART (July 25, 2016), http://www.takepart.com/article/2016/07/25/zero-days-stuxnet-iran [https://perma.cc/KP8G-A53T].

[311] Tran, *supra* note 165, at 393

[312] GEORGE LUCAS, ETHICS AND CYBER WARFARE: THE QUEST FOR RESPONSIBLE SECURITY IN THE AGE OF DIGITAL WARFARE 10 (2017).

between 2011 to 2013 for a cumulative 176 days.[313] A DDoS attack occurs when hackers use malicious programs to infect a series of networks or individual computers, called bots, and use the bots to overload a server — causing it to crash.[314]The event, collectively termed the "Ababil" or Swallows operation, aimed to crash the public-facing websites of forty-six financial institutions, including Bank of America, JPMorgan, the Nasdaq composite index, the New York Stock Exchange, and AT&T.[315] The damage cost faced by victim companies ran into tens of millions of dollars due to the severe interruptions of business activity achieved by the attacks.[316] At the same time, the hackers gained "unauthorized access into the Supervisor Control and Data Acquisition ("SCADA") systems of the Bowman Dam, located in Rye, New York."[317]

For reasons of optics, the group took its name from a prominent Muslim cleric and anti-colonialist active in the early twentieth century.[318] In a Twitter post, the group claimed responsibility and argued, "the attacks [were] launched in retaliation for the continued presence on YouTube of the American-made film *The Innocence of Muslims*" that portrayed Muslims in general, and the prophet Mohammed in particular, "in an unflattering light."[319] The group "vowed to continue [its] attacks until the U.S. President ordered the film removed from the Internet."[320] Yet contrary to their claims, the "Cyber Fighters of IZZ ad-Din al-Qassam" did not indiscriminately attack financial institutions.[321] Rather, the targets were carefully vetted and were primarily institutions that, "complied with the terms of the ongoing U.S. economic sanctions against Iran, part of the . . . effort to halt Iran's nuclear arms program."[322] Further, the anonymous Twitter account from which the group issued its demand to remove the film was the same that posted messages following an earlier cyberattack on the internal computer network of Aramco, the Saudi Arabian oil conglomerate.[323] Additionally, "[t]hose attacks . . . [supposedly accomplished by a different

[313] Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AM. J. INTL. L. 583, 598 (2018).

[314] Michael S. Urcuyo, *From Internet Trolls to Seasoned Hackers: Protecting Our Financial Interests from Distributed-Denial-of-Service Attacks*, 42 RUTGERS COMPUT. & TECH. L. J. 299, 302 (2016).

[315] Efrony & Shany, *supra* note 313, at 598. *See also* Press Release, Dept. of Justice at the U.S. Attorney's Office in the S.D.N.Y., Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Cyber Attacks (Mar. 24, 2016), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated [https://perma.cc/X9HG-TNGG].

[316] Efrony & Shany, *supra* note 313, at 598.

[317] *Id.*

[318] LUCAS, *supra* note 312, at 10.

[319] *Id.*

[320] *Id.*

[321] *Id.*

[322] *Id.*

[323] *Id.*

group] calling itself the 'Cutting Sword of Justice,' . . . erased data on all the affected drives, and inserted in their [stead a picture] of a burning American flag."[324] US security officials believe that, "both [cyber events] were acts of retaliation by Iranian state agents rather than [an] anonymous Islamic [digital] vigilante group."[325]

In March 2016, three years after the Ababil operation, the FBI gathered sufficient evidence to bring charges against seven Iranian hackers.[326] The cyber intrusions occurred against the backdrop of the U.S. and Iran negotiating a deal curbing Iran's nuclear-power ambitions.[327] Overall, the Obama Administration was cautious and largely defensive regarding the Ababil operation:

> Even a proposal by then National Security Agency (NSA) Director, Keith Alexander, to shut down the computer [systems] in Iran responsible for the DDoS attacks by a covert cyber operation [was seemingly rejected by officials] because [they] "were unsure that the action could be so precise and expressed concern that affecting a server in Iran—even if in self-defense—would represent a violation of its sovereignty" and [provoke] escalation.[328]

And the possibility "of using diplomatic back-channels was [likewise shelved because] it was [argued] that doing so might prompt the Iranians to intensify their attacks."[329] In turn, the Obama Administration's decision to refrain from an immediate, vocal, and firm response to stop the Ababil operation frustrated and undermined the helpless victim-institutions and led them to seriously consider self-help options like hack-backs against the attackers' servers.[330]

---

[324] *Id.*

[325] *Id.*

[326] U.S. Dep't of Justice Press Release, *supra* note 315.

[327] *See supra* text accompanying notes 304-306. Stuxnet was the "world's first real cyber weapon," and it is speculated that it was developed by the U.S. and Israel, although that has never been publicly confirmed. John J. Chung, *Nation-States and Their Cyber Operations in Planting of Malware in Other Countries: Is It Legal Under International Law?*, 80 U. PITT. L. REV. 33, 35-36 (2018). Unlike other worms or viruses, Stuxnet did not just hijack targeted computers or steal information, but instead physically destroyed equipment controlled by the computers. *See* Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History,* WIRED (July 11, 2011, 7:00 AM), https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/ [https://perma.cc/ZS84-FWN5]. In this manner, Stuxnet destroyed hundreds of centrifuges, which are necessary equipment to make weapons-grade uranium. *Id.*

[328] Efrony & Shany, *supra* note 313, at 600 (citations omitted).

[329] *Id.*

[330] *Id. See also* Michael Riley & Jordan Robertson, *FBI Probes if Banks Hacked Back as Firms Mull Offensives*, BLOOMBERG NEWS (Dec. 30, 2014), https://www.bloomberg.com/news/articles/2014-12-30/fbi-probes-if-banks-hacked-back-as-firms-mull-offensives (reporting on ongoing FBI investigation to discern if targeted banks hacked back Iranian servers); Nicholas Schmidle, *The Digital Vigilantes Who Hack Back*, NEW YORKER (May 7, 2018), https://www.newyorker.com/magazine/2018/05/07/the-

Hack-backs are "part of [the] concept of [digital] self-help or remediation [practices like] counterstrikes, 'active defenses,' . . . 'retaliatory hacking,' or 'offensive countermeasures.'"[331] A hack-back "might 'enable [an entity] to detect, trace, and actively respond to a threat [thereby] interrupting an attack in progress to mitigate [system damages].'"[332] Adding to its allure for private entities like financial institutions, a hack-back has the critical ability to forestall future attacks by defeating existing botnet structures.[333] The problem, however, is that despite the potential benefits, hack-backs may be unlawful because, ironically, due to the Computer Fraud and Abuse Act, "[t]he same laws that make it illegal to hack in the first place—for instance, to access someone else's system without authorization—*presumably* make it illegal to hack back."[334] Astonishingly, "[b]y some [metrics nearly] ninety percent of [U.S.] companies have been hacked."[335] In 2012, the then-director of the FBI Robert Mueller cautioned, "[t]here are only two types of companies: those that have been hacked and those that will be."[336] While agencies like the NSA defend government networks, "private [entities] are largely left to defend themselves on their own."[337] Not surprisingly, the private sector is increasingly relying upon cybersecurity firms, many of which are staffed by former NSA employees, to shore up cyber resilience plans.[338]

The evidence suggests Ababil was in retaliation for Stuxnet as well as to coax the U.S. to relieve sanctions pressure on Iran.[339] Increasingly, financial institutions are combating what to them feels like a war and they are "responding with an increasingly militarized approach."[340] Former government cyber

digital-vigilantes-who-hack-back (reporting that at least one targeted institution resorted to hacking back) [https://perma.cc/BV9W-U7FP].

[331] Sara Sun Beale & Peter Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16 DUKE L. & TECH. REV. 161, 190 (2018) (citations omitted). For an explanation of terms, *see* Sean L. Harrington, *Cyber Security Active Defense: Playing with Fire or Sound Risk Management?*, 20 RICH. J. L. & TECH. 1, 4 (2014).

[332] Beale & Berris, *supra* note 331, at 190.

[333] *Id.*

[334] 18 U.S.C. § 1030 (2012); PATRICK LIN, U.S. NAT'L SCI. FOUND., *ETHICS OF* HACKING BACK 4 (2016), http://ethics.calpoly.edu/hackingback.pdf [https://perma.cc/MG5Z-TMQA].

[335] Schmidle, *supra note 330.*

[336] *Id.*

[337] *Id.*

[338] *Id.*

[339] Jim Finkle & Rick Rothacker, *Exclusive: Iranian hackers target Bank of America, JPMorgan, Citi*, REUTERS (Sept. 21, 2012, 2:21 PM) https://www.reuters.com/article/us-iran-cyberattacks/exclusive-iranian-hackers-target-bank-of-america-jpmorgan-citi-idUSBRE88K12H20120921?feedType=RSS [https://perma.cc/C732-GTHR].

[340] Stacy Cowley, *Banks Adopt Military-Style Tactics to Fight Cybercrime*, N.Y. TIMES (May 20, 2018), https://www.nytimes.com/2018/05/20/business/banks-cyber-security-military.html [https://perma.cc/8MAK-AJJG].

intelligence and counterintelligence officials comprise the top echelon of banks' security teams and they bring to their new jobs fusion-style centers and threat analytics modeled against the internet's shadowy corners.[341] In the wake of President Trump's ending U.S participation in JCPOA and reinstituting severe economic sanctions, Iran became the number one "trending threat" at major U.S. banks.[342] John Hultquist, director of research at the leading cybersecurity firm FireEye, recently asserted, "Banks are taking a hard look at Iranian threat actors right now. We've advised all of our clients in the critical infrastructure space to consider the historic hostile actions of Iranian actors given [the return of sanctions]."[343] An appreciation of political realities and how cyber defenses might be adjusted accordingly is a critical step in the right direction. To this end, New York recently passed legislation aimed at narrowing the delta between AML/CFT regulatory schemes and OFAC foreign policy considerations while promoting enhanced cybersecurity measures[344]

C. NYDFS Regulations: A Model for America

The New York Department of Financial Services recently adopted a regulation that provides a greater level of structure to existing federal BSA and AML laws that pertain to New York state regulated institutions.[345] The regulation was created due to "'identified shortcomings in the transactions monitoring and filtering programs' of certain financial institutions" and to "a lack of [sufficient] governance, oversight, and accountability at senior levels."[346] Critically, Financial Services Regulation 504 ("Regulation 504") aims to fill a gap "in the current regulatory scheme promulgated by . . . current BSA/AML laws and regulations and [OFAC] requirements."[347] OFAC, an agency within the Department of Treasury, "administers and enforces economic and trade

---

[341] *Id.*

[342] Jose Pagliery, *US Banks Prepare for Iranian Cyberattacks as Retaliation for Sanctions*, CNN (Nov. 9, 2018), https://www.cnn.com/2018/11/09/tech/iran-sanctions-us-banks-cyber-hack-invs/index.html [https://perma.cc/MJ59-7AFF].

[343] *Id*. Economists posit the internet generates for the global economy between $2 - $3 trillion a year which means that perhaps as much as one-fifth of the internet's total value is disappearing due to illicit cyber events every 365 days. JOHN P. CARLIN, DAWN OF THE CODE WAR: AMERICA'S BATTLE AGAINST RUSSIA, CHINA, & THE RISING GLOBAL CYBER THREAT 32 (2018).

[344] Dixon, *supra* note 74, at 390. *See also* 3 N.Y. COMP. R. & REGS. tit. 3, § 504 (2016).

[345] 3 N.Y. COMP. R. & REGS. tit. 3, § 504 (2016). Regulated institutions include (1) "all banks, trust companies, private bankers, savings banks, and savings and loan associations chartered" in New York; (2) "all branches and agencies of foreign banking corporations licensed" in New York; and (3) "all check cashers and money transmitters licensed" in New York. *Id*. § 504.2.

[346] *DFS Final Regulation*, ERNST & YOUNG LLP (2016), https://www.ey.com/Publication/vwLUAssets/ey-dfs-final-regulation/%24FILE/ey-dfs-final-regulation.pdf [https://perma.cc/YS7L-CLNS].

[347] Dixon, *supra* note 74, at 390.

sanctions [predicated] on U.S. foreign policy and national security goals against targeted . . . regimes, terrorists," and others engaged in threats to national security.[348] Regulation 504 is comprised of three elements: (1) a transaction monitoring program, either manual or automated, which mandates regulated institutions monitor completed transactions to ratify compliance with anti-money laundering and BSA regulations;[349] (2) a watch list filtering program wherein regulated institutions interdict or intercept transactions made by entities that are prohibited from making such transactions by financial authorities such as OFAC;[350] and (3) an annual certification citing compliance to the Superintendent of the New York Department of Financial Services.[351] Ultimately, the Regulation 504 "enhances the security of [current] BSA/AML laws [and clarifies] the requirements and expectations for financial institutions."[352] Further, Regulation 504 makes explicit a significant shift in U.S. regulatory attitude: technology is a necessary component of AML monitoring.[353]

On August 28, 2017, the New York Department of Financial Services promulgated cybersecurity requirements for financial services companies.[354] Hailed as a unique and forward-leaning effort, Governor Cuomo asserted:

> New York, the financial capital of the world, is leading the nation in taking decisive action to protect our consumers and our financial system from serious economic harm that is often perpetrated by state-sponsored organizations, . . . terrorist networks, and other criminal enterprises. . . . This regulation helps guarantee the financial services industry upholds its obligation to protect consumers and ensure that its systems are sufficiently constructed to prevent cyber-attacks to the fullest extent possible.[355]

---

[348] *About: Terrorism and Financial Intelligence Office of Foreign Assets Control*, U.S. DEP'T OF TREAS. (Feb. 8, 2018), https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx [https://perma.cc/4VP2-BGE9].

[349] 3 N.Y. COMP. R. & REGS. tit. 3, § 504.3(a).

[350] *Id.* § 504.3(b).

[351] Dixon, *supra* note 74, at 397.

[352] *Id.* at 402.

[353] *NYS DFS Part 504 Breakdown and Analysis*, COMPLY ADVANTAGE (Feb. 22, 2017), https://complyadvantage.com/blog/nys-dfs-part-504-breakdown-analysis/ [https://perma.cc/4ECV-3DPY].

[354] *See generally Cybersecurity Requirements for Financial Services Companies (23 NYCRR 500)*, N.Y. ST. DEP'T FIN. SERVS. (2016), https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf [https://perma.cc/SYB3-N9GK].

[355] Press Release, Press Off. of Governor Andrew M. Cumo, *Governor Cuomo Announces Proposal of First-in-the-Nation Cybersecurity Regulation to Protect Consumers and Financial Institutions* (Sept. 13, 2016), https://www.governor.ny.gov/news/governor-cuomo-announces-proposal-first-nation-cybersecurity-regulation-protect-consumers-and [https://perma.cc/W4MK-ETXW].

A fundamental tenet of modern financial institutions is "AML is a significant component of cybersecurity, such that AML measures cannot be effective without cybersecurity," and cybersecurity at financial institutions cannot be accomplished without robust AML policies and procedures.[356] According to one compliance expert:

> Cybersecurity is intersecting in a new way with BSA/AML compliance, and it's becoming increasingly important that BSA/AML officers are aware of the kinds of cyberthreats out there. . . . There used to be a lot of silos out there, where compliance, risk management, network security, [were] separate parts, but today's cybersecurity environment means all those departments need to be interconnected in a new way.[357]

Technology is certainly part of the solution, but greater and better communication amongst BSA/AML/CFT and cybersecurity professionals within the government and private sector offers a long-term path to success. The past few years have seen progress toward this concept; for instance, on October 25, 2016, FinCEN issued a cyber threats advisory wherein it explained the proliferation of cyber events is a significant threat to the U.S. financial system.[358] Accordingly, FinCEN prompted financial institutions to use the well-known SAR reporting mechanism to report anomalous cyber events ("cyber SARs").[359] The rationale behind the cyber SAR is that information sharing between the government and private sector can help "guard against and report money laundering, terrorism financing, and cyber-enabled crime."[360] Traditionally, the cyber domain was foreign to BSA/AML teams in the private sector, and most departments lacked expertise and cross-training in the disciplines, but the FinCEN cyber SAR may help upend the longstanding but unhelpful paradigm.[361]

Recall the 176 days Iranian hackers targeted U.S. companies.[362] Critically, "[t]he NSA knew in advance [about Iran's] intent to penetrate the [financial

---

[356] Harry Dixon, *Maintaining Individual Liability in AML and Cybersecurity at New York's Financial Institutions*, 5 PENN ST. J.L. & INT'L AFF. 72, 104 (2017).

[357] *Cybersecurity, BSA Compliance More Interconnected Than Ever*, CREDIT UNION NAT'L ASS'N (Nov. 14, 2017), https://news.cuna.org/articles/113301-cybersecurity-bsa-compliance-more-interconnected-than-ever [https://perma.cc/HG3V-SRAX].

[358] *See Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime*, FINCEN (Oct. 25, 2016), https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf [https://perma.cc/46KV-6PUV].

[359] *Id*. at 1.

[360] *Id*.

[361] *See Integrating Cyber Incidents Into Your Anti-Money Laundering (AML) Program*, ACAMSTODAY (Sept. 18, 2018), https://www.acamstoday.org/integrating-cyber-incidents-into-your-anti-money-laundering-aml-program/ [https://perma.cc/3DCG-5DE4].

[362] Thomas Brewster, *U.S. Accuses 7 Iranians of Cyberattacks on Banks and Dam*, FORBES (Mar. 24, 2016) https://www.forbes.com/sites/thomasbrewster/2016/03/24/iran-hackers-charged-bank-ddos-attacks-banks/#7a459a6a7255 [https://perma.cc/J3TL-RT7G].

sector]."[363] According to former NSA deputy director Richard Ledgett, "the government has 'all kinds of visibilities and vantages' into" computer systems.[364] In the case of Iran, the NSA detected bots penetrating a server and forming a digital army of a sort used to wage DDoS attacks.[365] In March 2013, while the attacks were ongoing, a bank executive at JPMorgan proposed a hack-back to disable servers launching the Iranian attacks but the FBI opened an investigation into JPMorgan after agents found evidence some of the proposed sites were already targeted.[366] For Representative Tom Graves (R-GA), the situation had shades of the ridiculous: Iran hacked U.S. companies and now the FBI was investigating U.S. victims for possibly having taken defensive measures in the face of government inaction.[367] Representatives Graves, a member of the House Appropriations Subcommittee on Defense, has repeatedly argued the private sector requires a measure of latitude to protect themselves in the cyber domain.[368] A bill co-sponsored by Representative Graves, the Active Cyber Defense Certainty Act, would essentially enable private entities to advance into outside networks to gather intelligence and perform research on authorized intruders to determine attribution for cyber events.[369] Although the bill is flawed in many respects (*e.g.*, its language "contains large amounts of linguistic ambiguity that [could] defeat the [goal] of the legislation [and does not provide] sufficient legal protection for would-be defenders" or civil liability protection), its very existence speaks to the rising cyber threat to U.S. companies.[370]

VI. CONCLUSION

The U.S. stands at a crossroads. Will it forge a new world on its terms or succumb to a thousand cuts perpetrated by malicious actors across the globe? The current domestic and international AML and CFT regimes are insufficient. As America learned to its sorrow, devastating terrorist attacks can be inexpensive to action and terrorists are not easily targeted in this new world. The NYDFS Regulations offer hope by binding together American foreign policy and financial sector protections. Yet the government cannot foist a majority of responsibility on the private sector and proceed to abandon it in the face of

[363] Schmidle, *supra note 330* (reporting that at least one of the targeted banks resorted to hacking back).

[364] *Id*.

[365] *Id*.

[366] *Id.*

[367] *Id*.

[368] *Id.*

[369] Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. (2017). For a well-rounded discussion of the Active Cyber Defense Certainty Act, *see generally* Chris Cook, *Cross-Border Data Access and Active Cyber Defense: Assessing Legislative Options for a New International Cybersecurity Rulebook*, 29 STAN. L. & POL'Y REV. 205 (2018).

[370] *Id*. at 216.

attacks. Specifically, the NSA must do more to protect private sector industries, especially the financial sector. The avarice of China, the misdirection promulgated by Russia, and the nuclear ambitions of North Korea and Iran will not soon disappear. Education is certainly part of the answer; predictive analysis of threats is possible with sufficient knowledge of global events. In the mid-twentieth century, a famous maxim for a world at war was "loose lips sink ships" but in modern times a more appropriate slogan might be "communicate to protect." Until America learns to communicate across federal and state governments, across CI sectors and disciplines, it leaves itself vulnerable to continued attack.

As befits a new battlefield, the U.S. is bringing novel arms to bear. Financial institutions are in certain meaningful ways extensions of federal policies and agencies. Yet more needs to be done; an appreciation for the world as it is, a kind of twenty-first century *realpolitik*, is necessary to close the delta between existing regulation and what must be done to protect America in years to come.