Brooklyn Journal of International Law

Volume 45 | Issue 2 Article 1

6-1-2020

A Keystroke Causes a Tornado: Applying Chaos Theory to International Cyber Warfare Law

Daniel Garrie

Masha Simonova

A KEYSTROKE CAUSES A TORNADO: APPLYING CHAOS THEORY TO INTERNATIONAL CYBER WARFARE LAW

Daniel Garrie and Masha Simonova**

---

* B.A., (Comp. Sci. Brandeis Uni.), M.A., (Comp. Sci. Brandeis Uni), J.D., (Rutgers School of Law). Co-founder of Law & Forensics (www.lawandforensics.com). Neutral, Arbitrator, Mediator with JAMS. Adjunct Professor, Rutgers School of Law. Co-founder of UCLA Extension Global Cyber Institute. Email: daniel@lawandforensics.com. I am grateful for comments and discussions on earlier versions of this article from Chris Inglis, Gary Corn, Sarah Haines, Michael Mann, David Cass, Ella Garrie, Timothy Murphy, Judge Leo Gordon, Jim Eaglin, Yoav Griver, Leon Garrie, and my colleagues at JAMS, including Judge Gail Andler (ret.), Judge Judy Ryan (ret.), Judge Gregory Sleet (ret.), Andrew Nadolna, and Anne Lieu.

* J.D., Harvard Law School, Class of 2020. The authors thank the editors at the *Brooklyn Journal of International Law* for their careful and thoughtful edits to this article.

For want of a nail the shoe was lost.
For want of a shoe the horse was lost.
For want of a horse the rider was lost.
For want of a rider the message was lost.
For want of a message the battle was lost.
For want of a battle the kingdom was lost.
And all for the want of a horseshoe nail.

INTRODUCTION

Cyber warfare today finds itself on the front page of the news daily. Recent tensions between the United States (US) and Iran provide an example of how cyber warfare is different in kind from traditional, kinetic warfare. On June 22, 2019, the New York Times reported that US Cyber Command conducted cyberattacks against an Iranian intelligence group to which the US attributed prior attacks against oil tankers

near the Strait of Hormuz.[1] The attacks occurred on the same day that President Trump backed away from a conventional military strike on Iranian targets, but the cyber operation was allowed to proceed "because it was intended to be below the threshold of armed conflict."[2] This action was the first offensive use of force since Cyber Command was elevated to a full combatant command, and it reflects a new strategy called "defending forward."[3] The head of Cyber Command, General Paul Nakasone, defines this strategy as "operating 'against our enemies on their virtual territory.'"[4] It also reportedly reflects former National Security Advisor John Bolton's suggestion that the US is increasing its use of offensive cyber action or activity.[5] Coupled with these offensive attacks, the Department of Homeland Security warned that Iran was escalating cyber operations on US critical infrastructure and government agencies.[6] In August, the New York Times reported that Iran was still trying to recover information from the cyberattack.[7]

Haiyan Song, a technical expert from Splunk, has called the US cyber strike against Iran a "game changer," in that a "military action got diverted to really becoming a cyber action," displacing traditional means of warfare.[8] It is thus increasingly clear that the cyber domain demands more guidance; this is apparent from the President's statement indicating that using cyber was a means of bypassing standard kinetic warfare norms. Proposed solutions or emendations to this issue abound,

---

1. Julian E. Barnes & Thomas Gibbons-Neff, *U.S. Carried Out Cyberattacks on Iran*, N.Y. TIMES (June 22, 2019), https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html.

2. *Id.*

3. Ellen Nakashima, *Trump Approved Cyber-Strikes Against Iran's Missile Systems*, WASH. POST (June 22, 2019, 5:37 p.m. EDT), https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html?utm_term=.9e4de7649af7.

4. *Id.*

5. *Id.*

6. *Id.*

7. Julian E. Barnes, *U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say*, N.Y. TIMES (Aug. 28, 2019), https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html.

8. Karen Gilchrist, *US-Iran Cyber Strike Marks a Military 'Game-changer,' Says Tech Expert*, CNBC (July 2, 2019, 1:14 AM EDT), https://www.cnbc.com/2019/07/02/us-iran-cyber-strike-marks-a-military-game-changer-says-tech-expert.html.

but none adequately address the specific features of cyber warfare that set it apart from traditional kinetic warfare. This article argues that a new legal framework is necessary to properly address this problem, and such a doctrine should incorporate principles of chaos theory. As discussed more fully in Part IV, chaos theory is a branch of mathematics dealing with complex systems, with the most well-known example of chaos theory being the butterfly effect, which posits that a butterfly flapping its wings in Brazil can cause a tornado in Texas.[9] Similarly, a keystroke made in the United States can debilitate an Iranian intelligence agency.

Chaos theory has been deployed across many disciplines, demonstrating its capability for addressing modern, complex problems. For example, at the Massachusetts Institute of Technology (MIT) Center for Art, Science and Technology, an exhibit utilized chaos theory principles in visualizing oceanic movements.[10] The exhibit was a collaboration between Anastasia Azure, a Rhode Island School of Design–trained textile artist, and Larry Pratt, a Woods Hole Oceanographic Institution Senior Scientist and MIT/Woods Hole Joint Program teacher.[11] Pratt used chaos theory to "investigate the fluid pathways of eddies"[12] and to model turbulence, portraying the processes he used through photography and dance.[13] One piece used time-lapse photographs, depicting fluid pathways winding about a three-dimensional eddy.[14] Another involved a sculpture made from skeins of dyed fishing line, representing a cross-section of the eddy, as a study of the "complex forms" in nature.[15] These visualizations illustrate chaos theory's utility in analyzing and understanding complex, dynamic systems.

---

9. *See, e.g.*, Jamie L. Vernon, *Understanding the Butterfly Effect*, AM. SCIENTIST, https://www.americanscientist.org/article/understanding-the-butterfly-effect (last visited July 24, 2019).

10. Anya Ventura, *Ocean Stories: Visualizing Fluid Pathways*, ARTS AT MIT (June 26, 2013), https://arts.mit.edu/weaving-water/.

11. *Id.*

12. The National Oceanic and Atmospheric Administration defines an eddy as "a circular current of water." *What Is An Eddy?* NAT'L OCEANIC & ATMOSPHERIC ADMIN., https://oceanservice.noaa.gov/facts/eddy.html (last updated Nov. 13, 2019).

13. Ventura, *supra* note 10.

14. *Id.*

15. *Id.*

This article proceeds as follows: Part I summarizes notable instances of cyber warfare and other relevant attacks. It notes recent developments in artificial intelligence and autonomous weapons and how the proliferation of these systems impacts the cyber warfare landscape. Part II reviews the current state of international law governing cyber warfare. This part first discusses sources of international law, then describes the *Tallinn Manual* editions[16] and subsequent lack of state adoption. Part III examines why the cyber context is unique and calls for a new international law doctrine. Part IV then explains chaos theory and proposes using chaos theory principles to develop a solution to the inadequacy of current legal frameworks.

I. A SURVEY OF CYBER WAR

Part I surveys notable instances of cyber warfare throughout its short history. These attacks illustrate the complexity and severity possible in the cyber realm, as well as the difficulty of attribution. This part then addresses the proliferation of artificial intelligence and autonomous weapons and how these new tools will impact the ways in which cyber warfare is waged.

A. A Brief History of Cyber Warfare

In 1988, one of the first recognized worm viruses, the Morris worm, exploiting weaknesses in a particular Unix system, spread around computers mostly in the United States,[17] replicated itself, and brought computers to a halt.[18] Though not a warlike event, it was the advent of a new type of weapon. While cyberattacks consistently make news, rarely is one recognized as an act of actual cyber warfare. It would be a mistake, however, to overlook the rapid increase in sophistication and boldness of such attacks simply because they do not strike the pub-

16. The *Tallinn Manuals* are an analysis of the application of international law to the cyber domain. *See Tallinn Manual 2.0*, NATO COOPERATIVE CYBER DEF. CENTRE OF EXCELLENCE, https://ccdcoe.org/research/tallinn-manual/ (last visited Jan. 26, 2020).

17. *The History of Cyber Attacks – A Timeline*, NATO REV., https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm (last visited June 2, 2019).

18. *The Morris Worm: 30 Years Since First Major Attack on the Internet*, FBI NEWS (Nov. 2, 2018), https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.

lic imagination as applications of weaponry or an act of war.[19] With artificial intelligence and autonomous weapons beginning to affect the course of cyber warfare,[20] the time for planning is now.

In 2007, subsequent to a dispute between Estonia and Russia over the removal of a Soviet war memorial in Tallinn, unknown foreign intruders conducted a Distributed Denial of Service (DDoS) attack against Estonian government networks.[21] The attack rendered some online newspapers, government websites, and bank accounts inaccessible.[22] Moscow denied responsibility for the attack,[23] but Toomas Hendrik Ilves, president of Estonia at the time, called it "the first, but hardly the last, case in which a kind of cyber attack . . . was done in an overtly political manner."[24] The same year, unidentified foreign hackers breached US defense secretary Robert Gates' unclassified email account during a series of attacks on Department of Defense networks.[25] In 2010, Stuxnet, a complex, sophisticated worm that exploited zero-vulnerabilities in the Windows operating system to interfere with Siemens industrial control systems, was discovered in Iran, Indonesia, and elsewhere.[26] It was used

---

19. *See* Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 INT'L L. STUD. 99, 114–15 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) ("[A]fter a period of gestation . . . there is no insuperable difficulty in applying the general principles and rules of international law to the novel weapon (subject to some adjustments and adaptations, which crystallize in practice).").

20. *See* Part II.B, *infra*.

21. Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, GUARDIAN (May 16, 2007, 21:32 EDT), https://www.theguardian.com/world/2007/may/17/topstories3.russia; Emily Tamkin, *10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?*, FOREIGN POL'Y (Apr. 27, 2017, 8:30 AM), https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.

22. Tamkin, *supra* note 21.

23. *Id.*

24. *Id.* (internal quotation marks omitted).

25. David Morgan, *Pentagon E-mail System Breached*, REUTERS (Sept. 4, 2007, 4:17 AM), https://www.reuters.com/article/us-china-usa-hacking/pentagon-e-mail-system-breached-idUSPEK31756320070904; *The History of Cyber Attacks – A Timeline*, *supra* note 17.

26. Josh Fruhlinger, *What is Stuxnet, Who Created It and How Does It Work?*, CSO (Aug. 22, 2017, 2:39 AM PDT), https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html; *The History of Cyber Attacks – A Timeline*, *supra* note 17.

in an attack on Iran's nuclear program,[27] and it is now "widely accepted" that US and Israeli intelligence agencies developed Stuxnet and were responsible for the attack.[28] The group of researchers behind the *Tallinn Manual*[29] concluded that the attack was likely an illegal "act of force" under international law.[30]

Two years later, in 2012, the Russian cybersecurity firm Kaspersky Lab discovered a worldwide "cyber espionage network" called "Red October" that had been operating since at least 2007.[31] Hackers had deployed spear-phishing emails with attachments exploiting vulnerabilities in Microsoft Excel and Word to gain access to systems,[32] stealing data from smartphones, network equipment, and removable disk drives.[33] The attacks mainly targeted Eastern European and former Soviet and Central Asian countries, but some victims were in Western Europe and North America.[34] Diplomatic and government agencies were hardest hit, but Red October also reached research institutions, military installations, and energy providers, including nuclear and other critical infrastructures.[35] The same year, a DDoS attack dramatically slowed the websites of a number of US banks, including Bank of America, JPMorgan

---

27. Ellen Nakashima & Joby Warrick, *Stuxnet Was Work of U.S. and Israeli Experts, Officials Say*, WASH. POST (June 2, 2012), https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.0759dd1721da.

28. Fruhlinger, supra note 26; *see also* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

29. *See infra* Part III.B.

30. Shaun Waterman, *U.S.-Israeli Cyberattack on Iran Was "Act of Force," NATO Study Found*, WASH. TIMES (Mar. 24, 2013), https://www.washingtontimes.com/news/2013/mar/24/us-israeli-cyberattack-on-iran-was-act-of-force-na/.

31. GReAT, *The "Red October" Campaign – An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies*, KASPERSKY LAB (Jan. 14, 2013, 7:48 PM), https://securelist.com/the-red-october-campaign/57647/; *The History of Cyber Attacks – A Timeline*, *supra* note 17.

32. GReAT, *supra* note 31; Neil McAllister, *Surprised? Old Java Exploit Helped Spread Red October Spyware*, REG. (Jan. 16, 2013, 9:12 PM), https://www.theregister.co.uk/2013/01/16/red_october_java_connection.

33. GReAT, *supra* note 31.

34. *Id.*

35. *Id.*; *The History of Cyber Attacks – A Timeline*, *supra* note 17.

Chase, and Wells Fargo, making them "sporadically unreachable" for days.[36] The Islamist hacktivist group Izz ad-Din Al-Qassam Cyber Fighters, allegedly connected to Hamas, claimed responsibility for the attack, but US officials blamed Iran.[37]

In 2014, the computer systems of Sony Pictures were hacked by a group calling itself "Guardians of Peace." Employees' computers were locked and manipulated to display a skeleton image that read "Hacked by #GOP," with a message threatening the impending release[38] of employee names, job titles, addresses, and financial details, among other things.[39] Reports suggested that the US government suspected it was North Korea retaliating for Sony's planned release of *The Interview*, a comedy film about an assassination plot against Kim Jong Un.[40] Sony subsequently cancelled the release.[41] The FBI issued a corresponding accusatory statement noting similarities between the Sony hack and others attributed to North Korea.[42]

---

36. David Goldman, *Major Banks Hit With Biggest Cyberattacks in History*, CNN BUS. (Sept. 28, 2012, 9:27 AM ET), https://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html.

37. *Id.*; Warwick Ashford, *Izz ad-Din al-Qassam Hackers Launch Cyber Attack on US Bank Wells Fargo*, COMPUTER WKLY. (Sept. 27, 2012, 9:47), https://www.computerweekly.com/news/2240163994/Izz-ad-Din-al-Qassam-hackers-launch-cyber-attack-on-US-bank-Wells-Fargo; Ellen Nakashima, *Iran Blamed for Cyberattacks on U.S. Banks and Companies*, WASH. POST (Sept. 21, 2012), https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html?utm_term=.c54c2d3a1923.

38. Lori Grisham, *Timeline: North Korea and the Sony Pictures Hack*, USA TODAY (Dec. 18, 2014, 6:39 PM), https://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/ (last updated Jan. 5, 2015).

39. Aly Weisman, *A Timeline Of The Crazy Events In The Sony Hacking Scandal*, BUS. INSIDER (Dec. 9, 2014, 3:00 PM), https://www.businessinsider.com/sony-cyber-hack-timeline-2014-12; Sean Gallagher, *Sony Pictures hackers release list of stolen corporate files*, ARS TECHNICA (Nov. 26, 2014, 3:00 PM ET), https://arstechnica.com/information-technology/2014/11/sony-pictures-hackers-release-list-of-stolen-corporate-files/.

40. Andrea Peterson, *The Sony Pictures Hack, Explained*, WASH. POST (Dec. 18, 2014, 4:15 PM), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.0375c0b440e6.

41. *Id.*

42. Ellen Nakashima, *U.S. Attributes Cyberattack on Sony to North Korea*, WASH. POST (Dec. 19, 2014), https://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html?utm_term=.ff6ce4fda9bb.

Four iterations of a cyberattack—known as Shamoon 1, 2, 3, and 4—transpired between 2012 and 2017.[43] Under the "prevailing theory," they were carried out by a group of hackers sponsored by Iran.[44] In 2012, Shamoon 1 struck computer hardware infrastructure at the world's largest oil company, Saudi-Aramco, replacing the data on hard drives with an image of a burning American flag and wiping the memory on three-quarters of the company's computers.[45] The economic impact was massive. US Defense Secretary Leon Panetta called it "the most destructive attack that the private sector has seen to date."[46] Two weeks later, Shamoon 2 attacked the Qatari oil company RasGas with the same malware.[47] On November 17, 2016, Shamoon 3 hit crucial Saudi government agencies with another version that erased hard drives and displayed an image of the body of Alan Kurdi, a three-year-old Syrian boy who had drowned fleeing the Syrian civil war.[48] Shamoon 4 struck on January 23, 2017, a "digital time bomb, set in advance to explode at a specific time,"[49] infecting government and private computers in the Saudi kingdom in the same fashion as Shamoon 3.[50]

---

43. Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AM. J. INT'L L. 583, 620–21 (2018).

44. *Id.* at 622; *see also* Thom Shanker & David E. Sanger, *U.S. Suspects Iran Was Behind a Wave of Cyberattacks*, N.Y. TIMES (Oct. 13, 2012), https://www.nytimes.com/2012/10/14/world/middleeast/us-suspects-iranians-were-behind-a-wave-of-cyberattacks.html (discussing the 2012 Shamoon attack).

45. *See* Efrony & Shany, *supra* note 43, at 620–21.

46. Shanker & Sanger, *supra* note 44.

47. *See* Efrony & Shany, *supra* note 43, at 621. Although some analysts have characterized as Shamoon 2 the attack referred to in this Article as Shamoon 3, this article follows Efrony and Shany's characterization. *See, e,g.*, Robert Falcone, *Shamoon 2: Return of the Disttrack Wiper*, PALO ALTO NETWORKS (Nov. 30, 2016, 5:20 PM), https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/.

48. *See* Efrony & Shany, *supra* note 43, at 621; Jon Gambrell, *Saudi Arabia Warns Destructive Computer Virus Has Returned*, U.S. NEWS (Jan. 24, 2017, 9:36 AM), https://www.usnews.com/news/business/articles/2017-01-24/saudi-arabia-warns-destructive-computer-virus-has-returned.

49. Efrony & Shany, *supra* note 43, at 621.

50. *See* Gambrell, *supra* note 49; Perlroth & Krauss, *infra* note 64; Ms. Smith, *Saudi Arabia Again Hit with Disk-Wiping Malware Shamoon 2*, CSO (Jan. 24, 2017, 8:53 AM PST), https://www.csoonline.com/article/3161146/saudi-arabia-again-hit-with-disk-wiping-malware-shamoon-2.html.

In August 2016, a group calling themselves the "Shadow Brokers" started releasing stolen National Security Agency (NSA) hacking tools.[51] One of these tools, the 2017 WannaCry malware, used a flaw in the Windows operating system to encrypt data on hundreds of thousands of computers in over 150 countries and display a message demanding a ransom for the data, payable in Bitcoins.[52] Cybersecurity firms quickly identified technical footprints of the North Korea linked hacker group Lazarus,[53] and the NSA expressed "moderate confidence" that North Korea was responsible within a few weeks.[54] The United Kingdom (UK) government likewise officially attributed the attack to North Korea.[55] Also in 2017, computer systems in Ukraine were attacked by a version of the Petya ransomware (called NotPetya), which used the same stolen NSA tool to exploit an auto-update feature of a locally ubiquitous tax-calculation software.[56] Ukrainian companies, ATMs, and governmental agencies were infected, including departure boards at Boryspil International Airport in Kiev and the radiation monitoring equipment at the Chernobyl nuclear power plant.[57] NotPetya spread from there to over sixty countries.[58] Like Stuxnet and Shamoon, it was a "wiper malware" that caused "irreversible" damage.[59] Merck, FedEx, and Maersk, for exam-

---

51. *See* Scott Shane, Nicole Perlroth & David E. Sanger, *Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core*, N.Y. TIMES (Nov. 12, 2017), https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html.

52. Efrony & Shany, *supra* note 43, at 626.

53. *Id.* at 627.

54. Ellen Nakashima, *The NSA Has Linked the WannaCry Computer Worm to North Korea*, WASH. POST (June 14, 2017), https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html (internal quotation marks omitted).

55. *See* Karl Flinders, *UK Government Blames North Korea for WannaCry Cyber Attack*, COMPUTER WKLY. (Dec. 20, 2017, 9:01), https://www.computerweekly.com/news/450432112/UK-government-blames-North-Korea-for-WannaCry-cyber-attack.

56. *See* Efrony & Shany, *supra* note 43, at 628–29.

57. *See* Lizzie Dearden, *Ukraine Cyber Attack: Chaos as National Bank, State Power Provider and Airport Hit by Hackers*, INDEP. (June 27, 2017, 14:04), https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html.

58. *See* Efrony & Shany, *supra* note 43, at 629.

59. *Id.*

ple, suffered hundreds of millions of dollars in losses.[60] Cybersecurity experts have concluded with "high confidence" that Russia was responsible for NotPetya and that the attack was related to the ongoing armed conflict in Ukraine.[61]

On August 29, 2017, attackers targeted the Triconex industrial safety technology manufactured by Schneider Electric SE.[62] The technology was part of critical safety systems in nuclear, water, gas, oil, and chemical plants around the world.[63] Serious physical destruction would have resulted had it not been for "a bug in the attackers' computer code that inadvertently shut down the plant's production systems."[64] No official victim or attributing information has been released despite investigations by several US government agencies and private cybersecurity firms,[65] but according to the New York Times, the malware originated outside Saudi Arabia and targeted a chemical plant inside Saudi Arabia.[66] The New York Times report surmised that Iran was responsible due to its cyber capabilities and "presumed motive to harm Saudi Arabia," noting that it may have collaborated with another state.[67]

A cyberattack might not damage a system per se so much as it repurposes it into a harmful medium. On January 6, 2017, the Office of the Director of National Intelligence (ODNI) released *Assessing Russian Activities and Intentions in Recent US Elections*, a report that reflects the then-consensus of the CIA, FBI, and NSA that the Russian Federation interfered in

60. *See* Dan Gunderman, *NotPetya Costs Merck, FedEx, Maersk $800M*, CYBER SECURITY HUB (Oct. 31, 2017), https://www.cshub.com/attacks/news/notpetya-costs-merck-fedex-maersk-800m.

61. Efrony & Shany, *supra* note 43, at 629.

62. *Id.* at 622.

63. *Id.*; Samuel Gibbs, *Triton: Hackers Take Out Safety Systems in "Watershed" Attack on Energy Plant*, GUARDIAN (Dec. 15, 2017, 06:14 EST), https://www.theguardian.com/technology/2017/dec/15/triton-hackers-malware-attack-safety-systems-energy-plant.

64. Efrony & Shany, *supra* note 43, at 622; Nicole Perlroth & Clifford Krauss, *A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try*, N.Y. TIMES (Mar. 15, 2018), https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html.

65. Efrony & Shany, *supra* note 43.

66. Perlroth & Krauss, *supra* note 64.

67. Efrony & Shany, *supra* note 43 at 622–23; Perlroth & Krauss, *supra* note 64.

the 2016 US presidential election.[68] The report details alleged cyber activities, both covert and overt, and their possible motivations.[69] Together, these events should be understood as signals of a looming domain of warfare that demands change, adaptation, and the development of new practices. Otherwise, an unprecedented phase of cyber warfare may be impending, with nothing to steer away from triggering a total global war across cyber and kinetic fields.

B. Developments in Artificial Intelligence and Autonomous Weapons

Ongoing developments in artificial intelligence and autonomous weapons are also shaping the very understanding of the cyberwar landscape. Like a "flash" physical war—one that starts and uncontrollably escalates in seconds due to automation—"[a] flash cyberwar . . . is a real possibility. Automated hacking back could lead to escalation between nations in the blink of an eye."[70] As currently understood, the law does not distinguish between a deliberate action by a state actor and an act perpetrated by the state's autonomous machine. A state cannot escape responsibility merely because it deploys an autonomous weapon.[71]

One notable autonomous weapon is the US Navy's Aegis combat system. The Navy describes Aegis as a "centralized, automated, command-and-control (C2) and weapons control system that was designed as a total weapon system, from detection to kill."[72] In other words, it is "the electronic brain of a ship's weapons"[73] and is "built for flexibility."[74] Aegis is now in

---

68. OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, BACKGROUND TO "ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS": THE ANALYTIC PROCESS AND CYBER INCIDENT ATTRIBUTION (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

69. *Id.*

70. PAUL SCHARRE, ARMY OF NONE 229–30 (2018).

71. *See* Neil Davison, *A Legal Perspective: Autonomous Weapon Systems Under International Humanitarian Law*, INT'L REV. RED CROSS 5, 16 (UNODA Occasional Papers No. 30, 2017) ("Under the law of State responsibility, a State could be held liable for violations of IHL resulting from the use of an autonomous weapon system.").

72. *U.S. Navy Fact Sheet: AEGIS Weapon System*, U.S. NAVY, https://www.navy.mil/navydata/fact_print.asp?cid=2100&tid=200&ct=2&page=1 (last visited June 2, 2019).

73. SCHARRE, *supra* note 70, at 162.

use on over eighty warships.[75] Part of Aegis is a computer called Command and Decision that oversees the performance of the ship's radar and weapons.[76] Its decisions are governed by a series of statements, akin to programs, that the Navy calls "doctrine."[77] Aegis has a range of autonomy settings related to the "doctrine" statements, with different control levels for different threats.[78] The authority to activate the Aegis doctrine rests with the ship's captain,[79] so the automation level is "used to capture the ship captain's intent."[80]

According to Paul Scharre, Navy personnel have retained their human decision-making and caution in operating the Aegis system.[81] The system, however, illustrates that weapons with fully autonomous functions have already been deployed, in this case by six navies around the world.[82] Indeed, former Deputy Defense Secretary Robert Work has acknowledged the autonomy of Aegis, stating that it was programmed "to have a totally automatic setting, and literally the human at some point pushes the button and the machine makes all the decisions."[83] Work has also compared Aegis to automated "hacking back"[84] as part of a cyber-defensive strategy. Automation would be permitted, he says, "in defensive cases where all of the people who are coming at you are bad guys . . . [in] electronic war-

---

74. Thomas Karako, *Shield of the Pacific: Japan as a Giant Aegis Destroyer*, CSIS (May 23, 2018), https://www.csis.org/analysis/shield-pacific-japan-giant-aegis-destroyer.

75. SCHARRE, *supra* note 70, at 163.

76. *Id*. (internal quotation marks omitted).

77. *Id*.

78. *Id*. at 163–64.

79. *Id*. at 166.

80. *Id*. at 165.

81. *Id*. at 166–68.

82. *Aegis*, LOCKHEED MARTIN, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/aegis/Aegis-trifold.pdf (last visited June 2, 2019).

83. Kelsey D. Atherton, *Are Killer Robots the Future of War? Parsing the Facts on Autonomous Weapons*, N.Y. TIMES (Nov. 15, 2018), https://www.nytimes.com/2018/11/15/magazine/autonomous-robots-weapons.html (internal quotation marks omitted).

84. "Hacking back," also termed "active cyber defense," is the act of proactively responding to a cyber breach by hacking the intruder back. *See, e.g.*, Chris McDaniels, *Hacking Back: Revenge is Sweet, But is it Legal?*, SECURITY TODAY (Jan. 7, 2019), https://securitytoday.com/articles/2019/01/07/hacking-back.aspx.

fare, cyberwarfare, missile defense. . . . We will allow the machine to make essentially decisions . . . like, a cyber counterattack."[85]

Over ninety nations and non-state groups already possess drones.[86] Most of these are unarmed surveillance drones. At least sixteen countries retain armed drones, however, and a dozen or so others are in the process of arming their drones.[87] Drones are distinct from weapons in that they are reusable: they "can be launched, sent on patrol, and . . . return with their weapons unused if they do not find any targets."[88] But their proliferation also highlights how weapon systems with features to some degree removed from human decision-making are already part of modern warfare. And because autonomous weapons are themselves vulnerable to hacking, the consequences if a hostile state were to seize and redirect such a weapon would be unique, as the weapon would be in the adversary's hands.[89] The future of automation is thus cause for concern, particularly in cyberspace, given the rapid and unprecedented acceleration of innovation.[90]

II. THE CURRENT STATE OF CYBER WARFARE AND THE LAW—"GUERILLA WARFARE"

The current state of cyber warfare reflects a changing dynamic in the interpretation of what is and is not an act of war.[91] Acts of war were traditionally viewed as acts of a state.[92]

---

85. SCHARRE, *supra* note 70, at 228 (internal quotation marks omitted).

86. *Id.* at 56.

87. *Id.*

88. *Id.*

89. *Id.* at 222.

90. *See* THE WEAPONIZATION OF INCREASINGLY AUTONOMOUS TECHNOLOGIES: AUTONOMOUS WEAPON SYSTEMS AND CYBER OPERATIONS, UNIDIR 1 (2017), https://unidir.org/files/publications/pdfs/autonomous-weapon-systems-and-cyber-operations-en-690.pdf ("Autonomy-enhancing technological innovations in both physical and digital systems are advancing at a rapid pace.").

91. *See*, *e.g.*, Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 422 (2011); Michael N. Schmitt, *The Law of Cyber Warfare:* Quo Vadis*?*, 25 STAN. L. & POL'Y REV. 269, 294 (2014).

92. *See*, *e.g.*, Claire Oakes Finkelstein & Kevin H. Govern, *Introduction: Cyber and the Changing Face of War*, U. PA. FAC. SCHOLARSHIP, Paper 1566 (2015), https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=2567&context=faculty_scholarship.

Indeed, espionage has traditionally been a permitted behavior employed by states.[93] Asaf Lubin argues that states have a sovereign right to spy that "finds its underpinning in both historical and contemporary international law."[94] However, corporations are now increasingly representing state functions, impacting the determination of what is or is not an act of war; a corporation may now commit what was previously considered an act of war by a state. International law was not designed for this new paradigm.[95] Instead, lawyers and policy-makers are creating legal fictions spun out from existing law to protect private enterprises, stretching the law in a way that reflects the need to update the distinction between the roles of public and private actors.[96]

A. How is International Law Created?

The Restatement (Third) of Foreign Relations Law defines international law as "rules and principles of general application dealing with the conduct of states and of international organizations and with their relations inter se. . . ."[97] Accordingly, there are three primary sources of international law: custom, international agreements (treaties), and general principles. Customary law "results from a general and consistent practice of states followed by them from a sense of legal obligation."[98] International agreements "create law for the states parties thereto and may lead to the creation of customary international law when such agreements are intended for adherence by states generally and are in fact widely accepted."[99] Finally, general principles "common to the major legal systems, even if not incorporated or reflected in customary law or international

93. *See, e.g.*, Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 338 (1996).

94. Asaf Lubin, *Espionage as a Sovereign Right under International Law and Its Limits*, 24 ILSA Q. 22, 28 (2016).

95. *Id.*

96. *See*, *e.g.*, Daniel Garrie & Shane R. Reeves, *An Unsatisfactory State of the Law: The Limited Options for a Corporation Dealing with Cyber Hostilities by State Actors*, 37 CARDOZO L. REV. 1827 (2016).

97. RESTATEMENT (THIRD), OF FOREIGN RELATIONS LAW § 101 (AM. LAW INST. 1987).

98. *Id.* § 102(2).

99. *Id.* § 102(3).

agreement, may be invoked as supplementary rules of international law where appropriate."[100]

Jus ad bellum "refers to the conditions under which one may resort to war or to force in general" and strictly regulates the use of force under international law.[101] The United Nations (UN) Charter governs *jus ad bellum* and generally prohibits the threat or use of force by any state with just two recognized exceptions.[102] The first exception is the UN Security Council's right to "determine the existence of any threat to the peace, breach of the peace, or act of aggression" and power to "decide what measures shall be taken . . . to maintain or restore international peace and security." [103] The second exception ensures that states retain the "inherent" right of individual or collective self-defense if they are the victim of an armed attack.[104] The first exception is clearly of no avail to non-state actors, such as corporations responding to an anticipated state-sponsored cyber-attack.[105] The second exception expressly allows a victimized state to make an individual use-of-force determination in exercise of the inherent right of self-defense.[106]

The right of self-defense was a well-established international norm prior to the UN Charter and is generally recognized as part of customary international law.[107] The customary defini-

---

100. *Id.* § 102(4).

101. Robert Kolb, *Origin of the Twin Terms Jus Ad Bellum/Jus In Bello*, 320 INT'L REV. RED CROSS 553, 553 n.1 (1997); *see generally* Carsten Stahn, *'Jus ad bellum', 'jus in bello'. . . 'jus post bellum'? –Rethinking the Conception of the Law of Armed Force*, 17 EUR. J. INT'L L. 921 (2006) (tracing the historical origins of the doctrine).

102. *See* Christian J. Tams, *The Use of Force against Terrorists*, 20 EUR. J. INT'L L. 359, 360 (2009) (defining the two exceptions as "forcible enforcement measures within the framework of the organization's collective security system, and the right of self-defence against armed attacks"); Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 216 (2002) (defining the exceptions as "collective military action authorized by the U.N. Security Council, and . . . the long-standing international law principle of the right of self-defense").

103. U.N. Charter art. 39.

104. U.N. Charter art. 51.

105. *See* Jensen, *supra* note 102, at 217 ("the U.N. Charter authorizes the Security Council to determine the nature of a nation's actions and to decide what preventive or remedial actions are appropriate").

106. *Id.*; U.N. Charter art. 51.

107. Jensen, *supra* note 102, at 217.

tion, overwhelmingly cited as the *Caroline* doctrine, allows a state to use force if it "show[s] a necessity of self-defense; instant, overwhelming, leaving no choice of means, and no moment for deliberation."[108] But even if force is necessary, it cannot be "unreasonable or excessive, since the act, justified by the necessity of self-defense, must be limited by that necessity, and kept clearly within it."[109] Using force in self-defense, according to this customary definition, is therefore allowed if it is necessary and proportionate.[110] Customary international law thus gives states an independent authority to determine when it is necessary to exercise the inherent right to self-defense.[111]

The authority to engage in self-defense is broad and may include anticipatory uses of force to stymie an imminent armed attack.[112] There is an argument against this interpretation of Article 51, the ordinary language of which has led many to take the position that the Charter preempts (and restricts) the customary definition of self-defense.[113] Proponents of such an in-

---

108. Daniel Webster, *Letter to Henry Stephen Fox*, *in* 1 THE PAPERS OF DANIEL WEBSTER: DIPLOMATIC PAPERS 62 (K.E Shewmaker ed., 1983).

109. *Id.*

110. *Id.*; *see generally* Oscar Schachter, *The Right of States to Use Armed Force*, 82 MICH. L. REV. 1620, 1634–35 (1984); Oscar Schachter, *In Defense of International Rules on the Use of Force*, 53 U. CHI. L. REV. 113, 120 (1986); Oscar Schachter, *Self-Defense and the Rule of Law*, 83 AM. J. INT'L L. 259 (1989).

111. *See* W. Michael Reisman & Andrea Armstrong, *The Past and Future of the Claim of Preemptive Self-Defense*, 100 AM. J. INT'L L. 525, 548 n.111 (2006) (citing Thomas M. Franck, *What Happens Now? The United Nations After Iraq*, 97 AM. J. INT'L L. 607, 616 (2003)).

112. *See, e.g.*, Leo Van den hole, *Anticipatory Self-Defence under International Law*, 19 AM. U. INT'L L. REV. 69 (2003).

113. *See* Matthew Hoisington, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 B.C. INT'L & COMP. L. REV. 439, 449–50 (2009); Ryan Schildkraut, *Where There Are Good Arms, There Must Be Good Laws: An Empirical Assessment of Customary International Law Regarding Preemptive Force*, 16 MINN. J. INT'L L. 193, 202–04 (2007) (setting forth the "strict constructionist" position); *see generally* Robert J. Delahunty, *Paper Charter: Self-Defense and the Failure of the United Nations Collective Security System*, 56 CATH. U. L. REV. 871 (2007); Sean M. Condron, *Getting it Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J. L. TECH. 403, 412 (2007); Reisman & Armstrong, *supra* note 111, at 527–33; Sean D. Murphy, *The Doctrine of Preemptive Self-Defense*, 50 VILL. L. REV. 699, 706–11 (2005); Michael J. Glennon, *The Fog of Law: Self-Defense, Inherence, and Incoherence in Article 51 of the United Nations Charter*, 25 HARV. J.L. & PUB. POL'Y 539 (2002); Jason Barkham, *Information Warfare and In-*

terpretation, labelled "strict constructionists,"[114] point to the express condition that an "armed attack" should have occurred and that, even then, the "inherent right of individual or collective self-defence" is further subject to the express temporal limitation "until the Security Council has taken measures necessary to maintain international peace and security."[115] The essence of their concern is that any other result will tend to undermine the ban on the use of force.[116] On the other hand, adherents to the "imminent threat school"[117] on the meaning of Article 51 seize upon the Charter's likewise express provision that "nothing shall impair the inherent right" of self-defense, and on the absence of any limiting definition of an armed attack.[118]

In the aftermath of the US invasion of Iraq in 2003, a survey of International Court of Justice jurisprudence and state practice around the issue concluded that "if one were to hazard a prediction in this fluid situation, it would be that a conception of lawful self-defense incorporating only the *Caroline* doctrine will continue for most matters; beyond that, the right of self-defense will have been relaxed only for the so-called war against terrorism."[119] Duly acknowledging this tension as to what Article 51 can be taken to authorize should not impede a general consensus that an actual "armed attack" permits a proportionate response under the UN Charter, in self-defense and as a matter of inherent right, in response to a cyberattack.

Although "[t]here is clearly no common understanding of the application of Article 51 to [s]tate actions,"[120] states do have at least some authority to act proactively and offensively on self-defense grounds. If only states are permitted to carry out offensive cyber operations, however, then by reverse implication, a

---

ternational Law on the Use of Force, 34 N.Y.U. J. INT'L L. & POL. 57, 74–75 (2001).

114. Schildkraut, *supra* note 113, at 202.

115. U.N. Charter art. 51; *see* Schildkraut, *supra* note 113, at 202–04; *see generally* Malvina Halberstam, *The Right to Self-Defense Once the Security Council Takes Action*, 17 MICH. J. INT'L L. 229 (1996) (discussing positions on the "until" clause).

116. GEOFFREY S. CORN ET AL., THE LAW OF ARMED CONFLICT 20 (2018).

117. Schildkraut, *supra* note 113, at 205–07 (discussing the "the imminent threat school").

118. U.N. Charter art. 51; *see* Schildkraut, *supra* note 113, at 205.

119. Reisman & Armstrong, *supra* note 111, at 548.

120. CORN ET AL., *supra* note 116.

corporation is not seized of an inherent right of "self-defense" that would permit it to execute offensive cyber operations under the public international law that regulates state interactions.[121] "Article 2(4) [of the Charter] and its customary analog apply only to actions conducted by states or otherwise attributable to them pursuant to the law of state responsibility; it has no bearing on the actions of non-state actors. . . ."[122] As such, the inherent right of self-defense may well be a legal justification for state use of force in public international law, but for a corporation to invoke the same right as a transnational private actor, particularly in the case of a state adversary, is practically illogical.[123]

Academics and practitioners who advocate that corporations should be permitted to avail themselves of the right of self-defense are inviting wild scenarios that could threaten the UN Charter system of peace.[124] For example, Juan Zarate proposes that the "U.S. Department of Justice, Department of Homeland Security, and Treasury Department could create and issue special cyber warrants . . . to allow U.S. private sector actors to track and even 'hack back' or disrupt cyberattacks in certain instances to defend their systems."[125] Such hypotheticals

---

121. Garrie & Reeves, *supra* note 96.

122. DAVID LUBAN, JULIE R. O'SULLIVAN & DAVID P. STEWART, INTERNATIONAL AND TRANSNATIONAL CRIMINAL LAW 1028 (2018).

123. Garrie & Reeves, *supra* note 96, at 1856; *but see* JAN AMO HESSBRUEGGE, HUMAN RIGHTS AND PERSONAL SELF-DEFENSE IN INTERNATIONAL LAW 345–46 (2017) (discussing self-defense among private persons—or between these and state actors, even within the framework of public international law—as an important adjunct to the rule of law and state monopoly on violence, while noting the importance of limiting excessive self-help).

124. *C.f.* WYATT HOFFMAN & ARIEL E. LEVITE, PRIVATE SECTOR CYBER DEFENSE: CAN ACTIVE MEASURES HELP STABILIZE CYBERSPACE?, CARNEGIE ENDOWMENT FOR INT'L PEACE 9 (2017), https://carnegieendowment.org/files/Cyber_Defense_INT_final_full.pdf (defining cyber defensive actions as existing on a "spectrum," ranging from most passive to most aggressive); CENTER FOR CYBER & HOMELAND SECURITY, INTO THE GRAY ZONE: THE PRIVATE SECTOR AND ACTIVE DEFENSE AGAINST CYBER THREATS 19 (2016), https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReport FINAL.pdf (same).

125. JUAN C. ZARATE, THE CYBER FINANCIAL WARS ON THE HORIZON: THE CONVERGENCE OF FINANCIAL AND CYBER WARFARE AND THE NEED FOR A 21ST CENTURY NATIONAL SECURITY RESPONSE, FOUND. DEF. DEMOCRACIES 24 (2015), https://application-production.cdn.ranenetwork.com/blog/wp-content/uploads/2015/07/Cyber_Financial_Wars.pdf.

demonstrate that, if the legitimacy of public international law was available to non-state actors—such as corporations—such that they could readily justify a use of force as a matter of self-defense against a state actor, it would open the door for arbitrary, essentially uncontrolled applications of force.[126]

By contrast, Daniel Garrie and Shane Reeves have previously proposed an intermediary approach to the government-corporation issue, in which the government permits the corporation to deploy only self-help measures, such as remediating breaches and identifying perpetrators.[127] Governments must express limits, however, on the corporation's ability to use countermeasures. First, "[d]omestic legislation delegating countermeasure authority to the corporation must expressly prohibit any actions that may be construed as a use of force."[128] Second, any authorization must expressly delineate the attribution criteria before use.[129] Corporations could only use countermeasures if there is "strong evidence of state sponsorship of cyber hostilities."[130]

---

126. *See* Shane Reeves, *To Russia with Love: How Moral Arguments for a Humanitarian Intervention in Syria Opened the Door for an Invasion of the Ukraine*, 23 MICH. ST. INT'L L. REV. 199, 228 (2014) (cautioning against departing from the UN Charter's methodology for regulating the use of force as it is "a form of protection from the brutality and savagery of aggressive war"); *see also* Dinstein, *supra* note 19, at 107 ("Establishing the genuine identity of the attacker – and attributing the act to the real (as distinct from apparent) actor – is a major challenge in the present stage of technological development."); *c.f.* Matthew J. Sklerow, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 7–8 (2009) ("'attribution problem' locks states into the response crisis" as states treat cyberattacks as a criminal matter); HOFFMAN & LEVITE, *supra* note 124, at 43 (proposing an "international code of conduct" for private parties engaged in active cyber defense).

127. *See* Daniel Garrie & Shane R. Reeves, *So You're Telling Me There's A Chance: How the Articles on State Responsibility Could Empower 12 Corporate Responses to State-Sponsored Cyber Attacks*, HARV. NAT'L SEC. J. ONLINE 1, 12 (2016), https://harvardnsj.org/wp-content/uploads/sites/13/2016/01/Garrie-and-Reeves-Non-State-Actor-and-Self-Defense.pdf.

128. *Id.*

129. *Id.* at 13.

130. *Id.*

B. Tallinn Manual—Setting the Rules that No One Seems to Follow

The pressing need for guidance on cyber defense led to an effort to determine how international law applies to cyberspace.[131] The NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, invited a group of independent experts on the law of armed conflict to produce a manual on how international law applies to cyber warfare, calling it the International Group of Experts (IGE).[132] The drafters, led by Professor Michael N. Schmitt,[133] included practitioners, academics, technical experts, observers from NATO's Allied Command Transformation,[134] US Cyber Command,[135] and the International Committee of the Red Cross.[136] Over several years, the IGE developed the *Tallinn Manual on the International Law Applicable to Cyber Warfare*.[137] The first edition did not examine or account for the concerns of the private sector. A second version, the *Tallinn Manual 2.0*, published in 2017,[138] did recognize the new paradigm of corporations engaging in what, for practical purposes, look like state actions of war.[139] It addressed, for example, the situation where a corporation would "hack back" if maliciously targeted by a state actor as a viola-

131. NATO COOPERATIVE CYBER DEF. CENTRE OF EXCELLENCE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 3–4 (Michael N. Schmitt ed., 2013) [hereinafter *Tallinn Manual*].

132. *Id.* at 1.

133. *Michael N. Schmitt*, U. TEX. SCH. L., https://law.utexas.edu/faculty/michael-n-schmitt/ (last visited Apr. 17, 2020).

134. *Tallinn Manual*, *supra* note 131, at 9.

135. *Id.*

136. *Id.* at xi.

137. The *Tallinn Manual* provides an analysis of the application of *jus ad bellum* and *jus in bello* in cyberspace, along with descriptions of unresolved issues. Kristen E. Eichensehr, *Tallinn Manual on the International Law Applicable to Cyber Warfare; Edited by Michael N. Schmitt*, 108 AM. J. INT'L L. 585, 585 (2014) (reviewing *Tallinn Manual*, *supra* note 131). It relies "on the Western and NATO-centric perspectives of its drafters," which "may hamper its acceptance" outside that sphere, such as in China or Russia, where visions for cyberspace may differ. *Id.* It is an "indispensable resource" despite that shortcoming. *Id.*

138. NATO COOPERATIVE CYBER DEF. CENTRE OF EXCELLENCE, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 3–4 (Michael N. Schmitt ed., 2017) [hereinafter *Tallinn Manual 2.0*].

139. *See, e.g.*, *id.* at 17–18.

tion of sovereignty.[140] *Tallinn 2.0* has not been adopted into state practice and apparently stands no chance of adoption, at least not until states understand their responsibility to protect and secure their infrastructure.[141] The link between a state's infrastructure and the legal quandary around the notion of private entities going it alone to engage a state actor in cyber warfare is that critical infrastructure—more specifically, its functioning and safety—necessarily implicates cyberspace in the modern era.[142] The potential for cyber actions to destroy critical infrastructure more obviously implicates traditional territorial sovereignty.[143] States will have difficulty drawing international rules of engagement unless and until they have defined their internal role in this arena.[144]

---

140. *See, e.g.*, *id.*

141. *See* Efrony & Shany, *supra* note 43, at 585 (finding that "there appears to be limited support in state practice for certain key Rules of the *Tallinn Manuals*, and that it is difficult to ascertain whether states accept the Tallinn Rules and wish them to become authoritative articulations of international law governing cyber operations."); *see*, *e.g.*, John J. Chung, *Nation-States and Their Cyber Operation in Planting of Malware in Other Countries: Is It Legal Under International Law?*, 80 U. PITT. L. REV. 33, 62–63 (2018) (setting forth competing views on the relationship between territorial sovereignty and cyberspace and grounding the disputed legal status of cyber operations within this lack of consensus); Michael N. Schmitt & Liis Vihul, *Sovereignty in Cyberspace: Lex Lata Vel Non?*, 111 AJIL UNBOUND 213, 217–18 (2017) (characterizing state sovereignty as a "normative firewall" that nations generally, but unwisely, have not rigorously extended to their cyberspace).

142. *See Tallinn Manual*, *supra* note 131, at 258 (defining cyberspace as the environment formed by physical and non-physical components of computer networks and their use).

143. *See* Edwin Djabatey, *U.S. Offensive Cyber Operations against Economic Cyber Intrusions: An International Law Analysis – Part I*, JUST SECURITY (July 11, 2019), https://www.justsecurity.org/64875/u-s-offensive-cyber-operations-against-economic-cyber-intrusions-an-international-law-analysis-part-i/ (noting that *Tallinn Manual 2.0* indicates consensus "that a cyber operation will breach the target State's sovereignty in two circumstances. First, if it causes damage to cyber infrastructure in that State. . . . Second, . . . if it amounts to interference with or an usurpation of one of the target State's inherently governmental functions.").

144. *C.f.* Brandon Valeriano & Ryan C. Maness, *International Relations Theory and Cyber Security*, *in* THE OXFORD HANDBOOK OF INTERNATIONAL POLITICAL THEORY 259, 267 (Chris Brown & Robyn Eckersly eds., 2018) (discussing governance relationships among public and private institutions in the cyber domain and citing the Internet Corporation for Assigned Names and Numbers as an example).

Finally, Microsoft President Brad Smith's call for a "Digital Geneva Convention"[145] is misplaced.[146] According to Smith, the Digital Geneva Convention would bring states together to "affirm international cybersecurity norms that have emerged in recent years, adopt new and binding rules and get to work implementing them" in order to "protect civilians on the internet."[147] Colonel David Wallace and Lt. Colonel Mark Visger argue that Smith's proposal, which is directed at the technology community, neglects to consider current international law frameworks and casts issues in ways that do not conform to these frameworks, thus failing to appreciate the steps necessary to ratify such a convention.[148] Moreover, as a private actor, Brad Smith does not speak for the interests of the United States, but for the interests of a private company.

III. WHY CYBER CALLS FOR NEW DOCTRINE

> *[I]n war, as in life generally, all parts of the whole are interconnected and thus the effects produced, however small their cause, must influence all subsequent military operations and modify their final outcome to some degree, however slight. In the same way, every means must influence even the ultimate purpose.*[149]

The *Tallinn Manual* drove dialog among academics, practitioners, and jurists all over the globe on the application of traditional public international law to the cyber warfare arena, which presents new challenges in armed conflict.[150] The economics of cyber war allow entities to engage on a limited budget with state-level capabilities, so long as they have talented

---

145. Brad Smith, *The Need for a Digital Geneva Convention*, MICROSOFT: ON THE ISSUES (Feb. 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

146. *See, e.g.*, David Wallace & Mark Visger, *Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community*, 6 J.L. & CYBER WARFARE 3 (2018).

147. Smith, *supra* note 145.

148. Wallace & Visger, *supra* note 146, at 9–10.

149. CARL VON CLAUSEWITZ, ON WAR bk. II 158 (Michael Howard & Peter Paret, eds. & trans., Princeton U. Press 1976) (1832).

150. *See* James E. McGhee, *Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy* 2 J.L. & CYBER WARFARE 64, 82–94 (2013); Oliver Kessler & Wouter Werner, *Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare*, 26 LEIDEN J. INT'L L. 793, 795–96 (2013).

cyber warriors.[151] Cyber warfare is distinct from insurgency,[152] though the two share the trait of low barriers to entry.[153] Specifically, insurgents lack the equivalent tools and capabilities as state aggressors—instead, insurgents leverage alternative tactics to hinder larger actors and magnify their limited resources.[154] An operational cyber team can operate on the level of a state actor for a sliver of the price of conventional military efforts.[155] The United States has recognized this reality. Indeed, Ann Cox, a program manager in the Department of Homeland Security's Cyber Security Division, explicitly acknowledged this in her 2018 statement that "[a]nyone who has an interest in doing malicious things, there's a very low barrier to entry," naming the price as "only a few hundred dollars."[156] The net effect of this new reality is that states must confront a much larger pool of sophisticated actors that frequently leverage the same systems to operate.[157] If accepted

---

151. *See*, *e.g.*, SCOTT J. SCHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS 143–44 (2014) (pricing various nefarious cyber services).

152. *But see* Samuel Liles, *Cyber Warfare: As a Form of Low-Intensity Conflict and Insurgency*, *in* 2010 CONFERENCE ON CYBER CONFLICT PROCEEDINGS 47 (Christian Czosseck & Karlis Podins eds. 2010), https://ccdcoe.eu/uploads/2018/10/Liles-Cyber-warfare-As-a-form-of-low-intensity-conflict-and-insurgency.pdf (finding explanatory power in an insurgency or low-level conflict model of cyber hostilities, especially when it comes to the target government protecting its legitimacy).

153. *Id.* at 55 (detailing insurgents' reliance on external funding); *c.f.* COLIN P. CLARK, TERRORISM, INC.: THE FINANCING OF TERRORISM, INSURGENCY, AND IRREGULAR WARFARE 136 (2015) (discussing garden-variety fraud as the entry-level financing mechanism; money laundering); *but see* Dorothy E. Denning, *Barriers to Entry: Are They Lower for Cyber Warfare?* 1 IO JOURNAL 6, 10 (2009), https://faculty.nps.edu/dedennin/publications/Denning-BarriersToEntry.pdf (examining the commonplace premise of low barriers and suggesting that the barriers to entry remain proportionate to the potential size of the effects).

154. *See* Liles, *supra* note 152, at 53–55.

155. *See* Oona A. Hathaway, *The Drawbacks and Dangers of Active Defense*, *in* 2014 6TH INT'L CONFERENCE ON CYBER CONFLICT 38, 41–42 (Pascal Brangetto, Markus Maybaum & Jan Stinissen eds., 2014), https://ccdcoe.eu/uploads/2018/10/CyCon_2014.pdf.

156. Daniel Terdiman, *U.S. More Vulnerable to Weaponized Cyberattacks Than You Think*, FAST COMPANY (Mar. 10, 2018), https://www.fastcompany.com/40542648/the-u-s-is-more-vulnerable-to-weaponized-cyberattacks-than-you-think.

157. *See* Scott D. Applegate, *The Dawn of Kinetic Cyber*, *in* 2013 5TH INT'L CONFERENCE ON CYBER CONFLICT 163, 164–65 (Karlis Podins, Jan Stinissen &

and viewed in connection with the public international legal construct around the use of force, this aspect of cyber warfare becomes a suitable terrain for an analysis from the standpoint of chaos theory.

Chaos theory pertains to mathematics, rather than the theory of conflict, but its essential meaning surfaced in the opening passage quoted from Carl von Clausewitz's 1832 treatise, *On War*.[158] The link between public international law and this mathematical concept is the potentially outsized impact of easily overlooked factors on the outcome of complex dynamics over time. This part highlights the reasons the cyber context calls for a legal framework conceived with that in mind, and Part IV elaborates on the relevance of chaos theory.

Cyber presents unique challenges that deviate from the experience of the framers of the UN Charter (or von Clausewitz, for that matter). Foremost among these are: (1) the barriers to warfare are orders of magnitude lower in cyber than when kinetic fighting and weaponry were solely at play; (2) cyber attack victims' abilities to make attribution determinations are practically nil, and, thus they are incentivized to make bolder moves; and (3) states must work with the private sector to ensure the security of their own critical infrastructure, both digital and physical. The critical difference between cyber and traditional war is that no state would hesitate to assign responsibility for the common defense of a state's geographical territory to the government.

These differences are addressed in turn.

A. Low Barriers to Entry

Barring limited historical examples, such as Black Hand's assassination of Archduke Franz Ferdinand that arguably precipitated World War I, insurgents and individuals have generally yielded force in an asymmetric fashion to states.[159] Cyber is different in that a skilled cyber operator or team of a few elite cyber operators can wield and deploy cyber weapons on par with a large state. This allows an ever greater number of

---

Markus Maybaum eds., 2013), https://ccdcoe.org/uploads/2018/10/CyCon_2013_Proceedings.pdf.

158. *See* VON CLAUSEWITZ, *supra* note 149.

159. Daniel E. Slotnik, *Franz Ferdinand, Whose Assassination Sparked a World War*, N.Y. TIMES (June 28, 2016), https://www.nytimes.com/interactive/projects/cp/obituaries/archives/archduke-franz-ferdinand-world-war.

non-state actors[160] to become actively involved, which in turn increases the likelihood that a given cyber act starts a cascade of mutual retaliations[161] that envelope multiple actors other than the first mover.[162] In addition, non-state actors' motivations often deviate and substantially diverge from those of state actors.[163] Moreover, the diversity and richness of attack modalities and the complex web of interactions between attackers and retaliators multiply the complexity and unpredictability of hostilities.[164]

Cyber is unique: the monetary costs a state incurs when conducting a cyber war do not correlate to the effects, meaning a state can incur nominal monetary costs and conduct a cyber campaign with outsized impact. Monetary costs reflect barriers to entry, covering "expenditures for weapons, training, tools, facilities, telecommunications, salaries, travel, and recruiting."[165] The effects refer to the "outcomes of an operation and include deaths, property damage, financial losses, service disruptions, decisions made, and actions taken."[166] As Dorothy Denning explains, costs, or barriers to entry, must be compared to their effects; when the costs of achieving the same outcome

160. *See* Emilio Iasiello, *Is Cyber Deterrence an Illusory Course of Action?*, 7 J. STRATEGIC SECURITY 54 (2014); *see generally* Peter Margulies, *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility*, 14 MELB. J. INT'L L. 496 (2013) (on the risk of retaliation and escalation); Roger Hurwitz, *Keeping Cool: Steps for Avoiding Conflict and Escalation in Cyberspace*, 14 GEO. J. INT'L AFF. (INT'L ENGAGEMENT ON CYBER III) 17 (2013), https://www.jstor.org/stable/43134319.

161. Iasiello, *supra* note 160; Margulies, *supra* note160; Hurwitz, *supra* note160.

162. Iasiello, *supra* note 160; Margulies, *supra* note 160; Hurwitz, *supra* note 160.

163. *See, e.g.*, Johan Sigholm, *Non-State Actors in Cyberspace Operations*, 4 J. MIL. STUD. 1, 11 (2013); Mike Walls, *Nation-State Cyberthreats: Why They Hack*, DARKREADING (Jan. 18, 2015, 10:30 AM), https://www.darkreading.com/informationweek-home/nation-state-cyberthreats-why-they-hack-/a/d-id/1318522.

164. *See* LUCAS KELLO, THE VIRTUAL WEAPON AND INTERNATIONAL ORDER 10 (2017) (noting "the empowerment of nontraditional and dissatisfied actors who can disrupt interstate dealings, a subject that many theorists omit from their security frameworks").

165. Denning, *supra* note 153, at 7.

166. *Id.*

in cyberspace are lower than in a kinetic domain, cyberspace becomes a uniquely accessible mode for operation.[167]

In short, cyber war has the potential to deliver a better "bang for the buck" for states. For example, the cost of launching a dozen Tomahawk missiles[168] at a train station to take it offline runs in the tens of millions of dollars, not including the cost of building the technology. By contrast, the cost of having a team of skilled cyber operators hack the train control systems and encrypt them so that the train station cannot allow trains in or out likely will not exceed a couple million dollars.[169]

In reality, the costs incurred in an engagement often go beyond mere money. For example, unlike in cyber operations, a state that launches a kinetic attack runs the very real risk of revealing itself and incurring a kinetic or sanction-driven response. In the cyber realm, a state or sophisticated bad actor can deploy a cyber operation from anywhere. Accordingly, an actor can launch an attack from a bedroom or bunker thousands of miles away from the target, with little physical presence or equipment on the ground. Kinetic operations, on the other hand, often require physical transportation of personnel and equipment to the target area—be it by land, sea, or air—costing substantial money and time.[170] Additionally, kinetic operations may involve losing the benefit of surprise. Moreover, deploying cyber weapons requires nominal knowledge and ex-

---

167. *Id.*

168. *See* Amanda Macias, *US Taxpayers Paid Millions of Dollars for the Airstrikes on Syria. Here's a Breakdown of Key Costs*, CNBC (updated Apr. 17, 2018, 11:54 AM), https://www.cnbc.com/2018/04/16/syria-airstrikes-cost-to-us-taxpayers.html.

169. For the costs of cyber weapons, see, e.g., *Stuxnet Code*, INTERNET ARCHIVE, https://archive.org/details/Stuxnet (last visited June 5, 2019) (providing Stuxnet for download); Chris Bing, *You Can Now Buy a Mirai-powered Botnet on the Dark Web*, CYBERSCOOP (Oct. 27, 2016), https://www.cyberscoop.com/mirai-botnet-for-sale-ddos-dark-web/ (describing the sale of malware on the dark web); Dan Patterson, *The Dark Web is Where Hackers Buy the Tools to Subvert Elections*, CBS NEWS (Sept. 26, 2018, 11:38 AM), https://www.cbsnews.com/news/campaign-2018-election-hacking-the-dark-web/ (describing the sale of malware used to subvert elections on the dark web); Dan Swinhoe, *How Much Does it Cost to Launch a Cyberattack?*, CSO (Feb. 20, 2019, 3:00 AM PDT), https://www.csoonline.com/article/3340049/how-much-does-it-cost-to-launch-a-cyberattack.html (discussing the overall costs of cyberattacks); PAULO SHAKARIAN, JANA SHAKARIAN & ANDREW RUEF, INTRODUCTION TO CYBER-WARFARE 4–6 (2013).

170. *See, e.g.*, Macias, *supra* note 168.

pertise beyond knowing how to operate a computer and use the Internet.[171] In contrast, using and deploying most kinetic weapons requires a substantial investment of time and money in the operators of a kinetic weapon to ensure that it is used effectively.[172]

The consequences for attackers also vary in the kinetic and cyber contexts. Attackers conducting cyber operations are much less likely to be captured or killed than individuals involved in a kinetic operation.[173] Cyber attackers are often protected from capture or arrest by international boundaries—this occurred with the members of Russia's military intelligence outfit now indicted in the United States.[174] In contrast, it may be taken as commonplace that soldiers on the ground, at sea, or in the air are at risk of being the targets of a lethal counterstrike.[175]

Finally, many cyberattacks, such as ransomware, spearfishing, and low-level Denial of Service (DoS)[176] attacks, are perceived to be relatively harmless in the sense that most attacks to date are not known to have resulted in death, and the damage has not been permanent. For instance, defaced websites have been quickly restored and normal traffic flow has re-

---

171. Alex Hern, *Cyber-attacks and Hacking: What You Need to Know*, GUARDIAN (Nov. 1, 2016, 9:14 EDT), https://www.theguardian.com/technology/2016/nov/01/cyber-attacks-hacking-philip-hammond-state-cybercrime.

172. Diana Olick, *An army of one carries a high price*, NBC NEWS (Oct. 21, 2002, 10:39:34 AM ET), http://www.nbcnews.com/id/3072945/t/army-one-carries-high-price/.

173. *See infra* Part III.B.

174. Joel Samuels, *If the 12 Indicted Russians Never Face Trial in the US, Can Anything Be Gained?*, CONVERSATION (July 17, 2018, 6:45 AM EDT), http://theconversation.com/if-the-12-indicted-russians-never-face-trial-in-the-us-can-anything-be-gained-99997.

175. Of course, this will not always hold, as those launching missiles from a remote location or dropping bombs from the air may well be safer than careless cyber operators or ones who are beset with a concerted effort to track them down.

176. "In a DoS attack, a perpetrator uses a single Internet connection to either exploit a software vulnerability or flood a target with fake requests—usually in an attempt to exhaust server resources (e.g., RAM and CPU). On the other hand, distributed denial of service (DDoS) attacks are launched from multiple connected devices that are distributed across the Internet." *Distributed Denial of Service (DDoS)*, IMPERVA, https://www.imperva.com/learn/application-security/denial-of-service/ (last visited Feb. 2, 2020).

sumed when DoS attacks stop.[177] Of course, the monetary costs to the aggrieved party are often substantial.[178] However, there is a difference in the attack psychology when choosing between defacing a website or ransoming FedEx infrastructure compared to aiming and shooting a gun or detonating a bomb, which is certain to kill, maim, and/or destroy property.[179] The above discussion shows that a state or sophisticated cyber attacker can perpetrate a cyber attack with fewer resources and less risk than a kinetic attack.

B. Attribution

Adjoining the above paradigm that "if you eat food, you are full"—there is no result-based distinction between going to McDonalds to spend a few dollars and Noma in Denmark to spend hundreds of dollars—there is also the complex and difficult issue of attribution.[180] Most skilled cyber operators actively attempt to obfuscate their identities from their targets for the obvious reason of not being punished and the often added benefit, if successful, of exacerbating tensions with a wrongly attributed third party.[181] Today, no "cyber DNA" easily or readily

---

177. *See generally* Hans de Bruijn & Marijn Janssen, *Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies*, 34 GOV'T INFO. Q. 1 (2017), https://doi.org/10.1016/j.giq.2017.02.007.

178. *See, e.g.*, Gunderman, *supra* note 60 and accompanying text; 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/.

179. Today, the possibility of large scale or any lethal cyberattacks, while possible, are not likely, but if such events did occur, it would potentially allow the aggrieved party to respond using kinketic force to defend and respond to the attacker.

180. SHAKARIAN, SHAKARIAN & RUEF, *supra* note 169, at 4–6; *see also* Scott J. Shackelford, *State Responsibility For Cyber Attacks: Competing Standards for a Growing Problem*, CCD COE CONFERENCE ON CYBER CONFLICT PROCEEDINGS 2010 197, 200, https://ccdcoe.org/uploads/2018/10/Shackelford-State-Responsibility-for-Cyber-Attacks-Competing-Standards-for-a-Growing-Problem.pdf ("The science of tracing cyber attacks is primitive at best."); *The Cyber Security Whodunnit: Challenges in Attribution of Targeted Attacks*, SYMANTEC (Oct. 3, 2018), https://www.symantec.com/blogs/expert-perspectives/cyber-security-whodunnit-challenges-attribution-targeted-attacks ("Attribution of cyber attacks has never been an exact science.").

181. *See* Jan Dyment, *The Cyber Attribution Dilemma: 3 Barriers to Cyber Deterrence*, SECURITY INTELLIGENCE (Dec. 28, 2018), https://securityintelligence.com/the-cyber-attribution-dilemma-3-barriers-to-cyber-deterrence/ (describing false flag operations).

exists to directly tie an attacker to an event. At best, a state with some luck, money, and talent can attribute an attack to a specific entity. This is significant in today's global stage as it provides a non-state cyber operator working in concert with a state both the leverage and power to influence global affairs.[182] The ability to influence world affairs was formerly in the hands of only the upper tier of state actors. One prominent example is the US-supported Contra war in Nicaragua against the Sandinistas in the 1980s.[183]

Given the above and the fact that a legitimate response to a cyberattack from a legal standpoint can include the use of kinetic weapons, this means that a cyber conflagration has the potential to break out into a full-scale armed conflict.[184]

C. Attack Surface

A third factor magnifying the unpredictability, volatility, and instability of potential hostilities in cyber conflicts is the reality that states are no longer defending their borders—instead, they are defending their entire critical infrastructures.[185] In most countries, capitalism of the past 150 years has transferred responsibility for critical infrastructure to private or pseudo-private hands.[186] Indeed, a March 2019 Ponemon Insti-

---

182. *See* Kelly Jackson Higgins, *Destructive and False Flag Cyberattacks to Escalate*, DARK READING (Mar. 28, 2018, 4:30 PM), https://www.darkreading.com/attacks-breaches/destructive-and-false-flag-cyberattacks-to-escalate/d/d-id/1331390.

183. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Merits, 1986 I.C.J. Rep. 14 (June 27, 1986).

184. *See* Tarah Wheeler, *In Cyberwar, There Are No Rules*, FOREIGN POL'Y (Sept. 12, 2018, 8:00AM), https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/.

185. The attack surface is defined as the "total sum of vulnerabilities that can be exploited to carry out a security attack." *Definition: Attack Surface*, TECHTARGET, https://whatis.techtarget.com/definition/attack-surface (last updated Feb. 2019).

186. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-39, CRITICAL INFRASTRUCTURE PROTECTION: PROGRESS COORDINATING GOVERNMENT AND PRIVATE SECTOR EFFORTS VARIES BY SECTORS' CHARACTERISTICS 2 (2006), https://www.gao.gov/assets/260/252603.pdf ("Because about 85 percent of the nation's critical infrastructure is owned by the private sector, it is vital that the public and private sectors work together to protect these assets.").

tute[187] report found that "[f]ew organizations have sufficient visibility into their attack surface."[188] This narrative, even if only partially valid, significantly impairs the ability of states to secure critical infrastructure because private and public actors tend to have completely different goals.

In a large number of countries, governments may lack the power and expertise to respond decisively to an attack on critical infrastructure at the scale of the whole state, whether the attack is initiated by another state or any other type of actor.[189] The UK, Germany, Australia, and the Netherlands, for example, have all previously blamed Russia for a worldwide cyber campaign targeting various governmental agencies, companies, media, and sports entities, yet these attacks persist.[190] Moreover, there is not yet an international law consensus that an attack on critical infrastructure with no "violent" effects constitutes an impermissible use of force permitting self-defense.[191]As the Russia example demonstrates, until states, from a governance or administrative perspective, define a way of protecting critical infrastructure against cyber threats, the issue of defense against and response to cyberattacks from a military or security perspective—which is the public interna-

187. The Ponemon Institute "conducts independent research on data protection and emerging information technologies." *Ponemon Institute,* PONEMON INST., https://www.ponemon.org/ (last visited Feb. 2, 2020).

188. CYBERSECURITY IN OPERATIONAL TECHNOLOGY: 7 INSIGHTS YOU NEED TO KNOW, PONEMON INSTITUTE (Mar. 2019), https://lookbook.tenable.com/ponemonotreport/ponemon-OT-report.

189. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-18-211, CRITICAL INFRASTRUCTURE PROTECTION: ADDITIONAL FRAMEWORKS ARE ESSENTIAL FOR ASSESSING CYBERSECURITY FRAMEWORK ADOPTION (Feb. 2018) (finding that US government entities (1) "[m]ay be limited in their ability to commit necessary resources towards [National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*] adoption"; (2) "[m]ay not have the necessary knowledge and skills to effectively implement the framework"; (3) "[m]ay face regulatory, industry, and other requirements that inhibit adopting the framework"; and (4) "[m]ay face other priorities that take precedence over conducting cyber-related risk management or adopting the framework").

190. *See Germany Warns Russia Over Cyberattacks*, DW (Oct. 5, 2018), https://www.dw.com/en/germany-warns-russia-over-cyberattacks/a-45767953; *UK, Australia Blame Russia for Series of Global Cyberattacks*, DW (Oct. 5, 2018), https://www.dw.com/en/uk-australia-blame-russia-for-series-of-global-cyberattacks/a-45745308.

191. Waxman, *supra* note 91, at 435–36.

tional law framework for the use of force—will remain unresolved.

IV. NEW LEGAL DOCTRINES FOR CYBER WARFARE SHOULD INCORPORATE CHAOS THEORY

These unique features of cyber hostilities demonstrate the necessity of a new approach to the development of cyber warfare law. The law is currently built for traditional, kinetic warfare, rather than for far less predictable cyberattacks. International law, in particular, is built around customary norms and treatises that do not consider the issues cyber warfare presses.[192] The legal structures need to change to account for these challenging novel circumstances. This section proposes that such an update can and should draw on the principles of chaos theory in addressing the challenge. Chaos theory is superior to traditional conceptions of kinetic warfare and offers the best lens through which to understand cyber warfare.

A. What Is Chaos Theory?

Chaos theory deals with complex systems. It originally constituted a shift away from Newtonian linear and sequential physics suited to the study of nonlinear, unpredictable, and dynamical systems.[193] Indeed, chaos theory posits that a "Newtonian vision of an orderly universe no longer exists."[194] Whereas causation has a "proportionate relationship" in Newtonian linear systems, it is "not proportionate" in nonlinear systems, and the mathematical relationship "between variables is dynamic, rather than stable."[195] Chaos theory therefore states that small "changes to the starting variables of a nonlinear dynamic sys-

192. *See supra* Parts III & IV.

193. *See* Robert Bishop, *Chaos*, STAN. ENCYCL. PHIL. (Edward N. Zalta ed., 2017), https://plato.stanford.edu/archives/spr2017/entries/chaos/.

194. Toby J. Tetenbaum, *Shifting Paradigms: From Newton to Chaos*, 26 ORGANIZATIONAL DYNAMICS 21, 24 (1998).

195. Vincent Di Lorenzo, *Legislative Chaos: An Exploratory Study*, 12 YALE L. & POL'Y REV. 425, 430 (1994). Dynamic systems "exhibit a complicated, apparently random-looking behavior." Aristides Dokoumetzidis, Athanassios Iliadis, & Panos Macheras, *Nonlinear Dynamics and Chaos Theory: Concepts and Applications Relevant to Pharmacodynamics*, 18 PHARMACEUTICAL RES. 415, 415 (2001).

tem will produce highly varied results[,] and the variables describing the state of the system will not repeat predictably."[196]

1. The Butterfly Effect and Fractals

The most well-known principle of chaos theory is the "butterfly effect." The butterfly effect emerged out of Edward Lorenz's idea that a butterfly flapping its wings in one part of the world could cause a tornado in another part.[197] A mathematician and meteorologist at MIT, Lorenz was researching weather patterns when he stumbled upon what became the basis for the butterfly effect.[198] In 1960, working with a computer program that simulated weather conditions using twelve variables comprised of equations expressing relationships, such as that between temperature and pressure, he examined printouts from the machine marking the passage of days and modeling the weather on each day.[199] The results showed repetition, but they were "never quite exact"—there was an "orderly disorder."[200] One day in early 1961, Lorenz took a "shortcut," whereby he started the machine midway through and manually entered the numbers for the machine's initial conditions.[201] He left for a cup of coffee and when he returned, he noticed a wide divergence between the new and old printouts.[202] While manually inputting the values of the variable, he had rounded off the earlier-used number from .506127 to .506,[203] thinking a difference of one part in a thousand immaterial. Instead, he found the slight divergence had in fact dramatically altered the machine's weather output.[204] This accidental result led him to the

196. Jason S. Collins, *"Pockets of Chaos": Management Theory for the Process of Computer Security*, SANS INST. (Nov. 12, 2001), https://www.sans.org/reading-room/whitepapers/infosec/pockets-chaos-management-theory-process-computer-security-602.

197. JAMES GLEICK, CHAOS: MAKING A NEW SCIENCE 8 (Penguin Books, 1987); Peter Dizikes, *When the Butterfly Effect Took Flight*, MIT TECH. REV. (Feb. 22, 2011), https://www.technologyreview.com/s/422809/when-the-butterfly-effect-took-flight/.

198. GLEICK, *supra* note 197, at 16; Dizikes, *supra* note 197.

199. GLEICK, *supra* note 197, at 11–12.

200. *Id.* at 15.

201. *Id.* at 16.

202. *Id.*; Dizikes, *supra* note 197.

203. GLEICK, *supra* note 197, at 16; Dizikes, *supra* note 197.

204. GLEICK, *supra* note 197, at 16.

insight that came to be known as the butterfly effect.[205] The butterfly effect's technical name, "sensitive dependence on initial conditions," echoes the meaning of the *For want of a nail* proverb recited at the beginning of this article.[206]

Lorenz demonstrated this principle of complexity through various equations.[207] One example the equations describe is a water wheel in which water drips into evenly spaced containers on the wheel.[208] If the water drips slowly, the top bucket does not fill up, and the wheel never starts turning; but if it flows faster, the weight of the top bucket starts the wheel moving, and it will turn at a steady rate.[209] If the water flows even faster, however, the spin becomes chaotic due to innate nonlinear effects in the system.[210] If the wheel spins quickly, the buckets will not fill up significantly and can start up the other side of the wheel before they have time to empty.[211] Accordingly, heavy buckets on the side moving upwards can cause the wheel to slow down and reverse direction. Lorenz found that, over long periods of time, the wheel can reverse repeatedly.[212]

Indeed, scientists later suggested that this kind of behavior may provide an explanation for the earth's magnetic field, which has flipped throughout history, often "at intervals that seem erratic and inexplicable."[213] Lorenz's equations demonstrated a complex system known as a "strange attractor," with the specific dynamics his equations covered deemed the "Lorenz attractor," graphed in the shape of butterfly wings.[214] The shape demonstrates that "almost all chaotic phenomena can vary only within limits."[215] Most strange attractors have a

---

205. Dizikes, *supra* note 197.

206. GLEICK, *supra* note 197, at 23.

207. *See* Edward N. Lorenz, *Deterministic Nonperiodic Flow*, 20 J. ATMOSPHERIC SCIENCES 130 (1963). As of April 17, 2020, Google Scholar shows that this article has been cited 22,071 times.

208. GLEICK, *supra* note 197, at 27.

209. *Id.*

210. *Id.*

211. *Id.*

212. *Id.*

213. *Id.* at 29.

214. I*d.* at 28–29, 140; Paul Halpern, *Chaos Theory, The Butterfly Effect, And The Computer Glitch That Started It All*, FORBES (Feb. 13, 2018, 10:00 AM EST), https://www.forbes.com/sites/startswithabang/2018/02/13/chaos-theory-the-butterfly-effect-and-the-computer-glitch-that-started-it-all/#66bc002469f6.

215. Dizikes, *supra* note 197.

structure the mathematician Benoit Mandelbrot later named a "fractal."[216] In a fractal, the "same structure and behavior appears on a variety of scales."[217] Accordingly, fractals are a fitting visual representation of the functioning of chaos theory.[218]

In sum, chaos theory has five main facets. First, there are many forces interacting to create change.[219] Second, sensitive dependence on initial conditions means that small changes in initial conditions multiply over time so the "cumulative result is a large difference in outcome."[220] Third, "changes occurring in physical systems are nonlinear in character." [221] Fourth, change is "aperiodic," meaning that the point at which the system will settle is unpredictable.[222] Finally, natural systems exist in an environment "itself in flux."[223]

2. Application to Cyber Warfare

The above brief description of chaos theory can be aptly mapped onto cyber systems. Scholars have already suggested applying chaos theory in, for example, causation analysis,[224] zoning,[225] financial markets and corporate law,[226] organized

---

216. Halpern, *supra* note 214; William Harris, *How Chaos Theory Works*, HOWSTUFFWORKS (Mar. 2, 2014), https://science.howstuffworks.com/math-concepts/chaos-theory.htm.

217. Halpern, *supra* note 214.

218. Collins, *supra* note 196; Di Lorenzo, *supra* note 195, at 431.

219. Di Lorenzo*, supra* note 195, at 430.

220. *Id.*

221. *Id.*

222. *Id.* at 431.

223. *Id.*

224. Edward S. Adams, Gordon B. Brumwell, & James A. Glazier, *At the End of Palsgraf, There is Chaos: An Assessment of Proximate Cause in Light of Chaos Theory*, 59 U. PITT. L. REV. 507, 542 (1998). In *Massachusetts v. EPA*, however, Justice Roberts scoffed at chaos theory principles in the standing context. 549 U.S. 497, 546 (2007) (Roberts, J., dissenting) (arguing that the Court's analysis neglects to address how the regulation at issue will redress the alleged injury: "Schoolchildren know that a kingdom might be lost 'all for the want of a horseshoe nail,' but 'likely' redressability is a different matter.").

225. *See* John Mixon & Kathleen McGlynn, *A New Zoning and Planning Metaphor: Chaos and Complexity Theory*, 42 HOUS. L. REV. 1221 (2006).

226. *See, e.g.*, Steven L. Schwarcz, *Regulating Complexity in Financial Markets*, 87 WASH. U. L. REV. 211 (2009); Lawrence A. Cunningham, *From Random Walks to Chaotic Crashes: The Linear Genealogy of the Efficient Capital Market Hypothesis*, 62 GEO. WASH. L. REV. 546 (1994).

crime,[227] electronic health information privacy,[228] and legislative dynamics.[229] The unique features of cyber warfare set forth above make it an appropriate field in which to apply chaos toward the invention of new legal doctrines to govern its conduct. Indeed, as David Brumley, a computer scientist at Carnegie Mellon University and CEO of ForAllSecure, has stated in discussing computer security and autonomous cyber systems, "I tend to view everything as a system—a dynamic system."[230] When advising someone on cyber war, one cannot take a linear approach. Instead, legal advisors should consider the myriad potential outcomes that may occur as a result of a dynamic system. Three principles are thus useful to consider for applying chaos theory to the international legal framework.

B. Three Principles for Applying Chaos Theory to International Cyber Warfare Law

This Article proposes three principles for the application of chaos theory to the development of international cyber warfare law. First, not all actions in the cyber realm are created equal, and the effects of different actions can range in a manner similar to the butterfly effect. Second, cyber warfare is an equalizer, permitting access to a wide range of actors. Third, the traditional application of norms to the cyber warfare context does not work because repetitive behavior is not to be expected and attribution is often difficult if not impossible.

1. Not All Actions in the Cyber Realm are Created Equal, and They Can Produce Disparate Effects.

Not all actions taken in cyber space are equivalent to a bullet fired in kinetic warfare. Rather, the butterfly effect applies, il-

---

227. *See* Julie Beesley, *Organised Chaos: Seeing with New Eyes*, 21 CURRENT ISSUES CRIM. JUST. 343, 350–51 (2010).

228. *See* Kathryn McEnery, *The Usefulness of Non-Linear Thinking: Conceptual Analysis Tools and an Opportunity to Develop Electronic Health Information Privacy Law*, 23 HEALTH LAW. 18, 28 (2010).

229. *See* Di Lorenzo, *supra* note 195.

230. SCHARRE, *supra* note 70, at 217, 227; *see also* Gary Corn, *Tallinn Manual 2.0 – Advancing the Conversation*, JUST SECURITY (Feb. 15, 2017), https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/ (arguing that "the uniqueness and rapidly evolving nature of cyberspace will place adaptive pressure on most of the existing international law framework").

lustrating how one small network vulnerability may be exploited to an increasingly sizeable effect. Sensitive dependence on initial conditions is also fundamentally important in the autonomous weapons context, where, for example, an accidental decision by an Aegis operator to permit the system to run using fully automated doctrine might be the flap of the butterfly's wings that causes a tornado.[231] Additionally, as seen in the discussion on attribution in Part III, sensitive dependence on initial conditions is also evident in the context of attribution at the strategic, tactical, and operational levels: if a tactical threat analyst mistakenly permits cognitive bias to color their attribution analysis, a strategic threat actor further up the organizational chain may make a business decision having a significantly broader impact.[232]

Moreover, advisors attempting to provide guidance to a cyber operator will not always have the complete picture of the adversary's systems. Accordingly, it may not be clear, based on the initial conditions that the operator employs in Country A, what effect the acts will have on Country B. In this chaotic system, a small change in these initial conditions could correspond with the production of a significant change in effect on Country B's systems. Advisors would therefore be remiss to not deploy a chaos theory analysis in analyzing the international law implications of conducting certain operations.

2. Cyber Warfare is an Equalizer

A cyber weapon that is the equivalent of a nuclear weapon in kinetic warfare is within the reach of any state.[233] As discussed in Part III, low barriers to entry are a unique feature of the cyber domain.[234] The multiplicity of actors, their differing motivations, and diverse attack modalities in the cyber context combine to render hostilities increasingly complex and unpredictable.[235] Accordingly, international law needs a device or mechanism by which to account for the equalized nature of the cyber threat. Traditional, now simplistic-seeming conceptions of warfare are not apt to handle the complexity of current or

231. *See supra* notes 72–85 and accompanying text.
232. *See supra* Part IV.B.
233. *See supra* Part IV.A.
234. *Id.*
235. *See supra* Part IV.

foreseeable developing cyber hostilities. Indeed, this is reflected in the lack of state adoption of some of the key rules in the *Tallinn Manual*.[236] Until the proposed legal rules reflect the real nature of the threat, this rejection of standardized rules will likely continue.

3. The Concept of Dynamic Systems in Chaos Theory Must be Applied to International Cyber Warfare Law Because Norms are Inapplicable, and Attribution is a Fiction.

International law has traditionally focused on norms, which inherently depend on repetitive behavior.[237] In the cyber realm, repetitive behavior is not to be expected, much less relied upon, due to the evolving nature of the threat and the broad attack landscape.[238] For example, each time cybersecurity experts think that they have pinned down Petya malware, it turns out that NotPetya has proliferated.[239] The privatization of critical infrastructure also means that the attack surface is increasingly diverse.[240] Moreover, international norms are only effective when attribution is possible and definite, but, as discussed in Part IV, attribution cannot be expected with certainty in the cyber context.[241] Indeed, the idea of useful attribution is practically fantastical when it comes to sophisticated actors.[242] Every response to a cyberattack must therefore be measured against a new, dynamic risk analysis.[243] Because of the presently in-

---

236. *See supra* note 141 and accompanying text.

237. *See* Myres S. McDoual & W. Michael Reisman, *The Prescribing Function in World Constitutive Process: How International Law Is Made*, 6 YALE STUD. WORLD PUB. ORD. 249, 263, 273 (1980); Andrew T. Guzman, *A Compliance-Based Theory of International Law*, 90 CALIF. L. REV. 1823, 1837 (2002) (citing Harold H. Koh, *Transnational Legal Process*, 75 NEB. L. REV. 181, 183–84 (1996).

238. *See* Corn, *supra* note 230 (noting the "hyper-dynamic and evolving nature of cyberspace").

239. *See* Efrony & Shany, *supra* note 43, at 628–29.

240. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 186.

241. *See supra* Part IV.B; *but see* Jon R. Lindsay, *Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack*, 1 J. CYBERSECURITY 53, 61 (2015), https://doi.org/10.1093/cybsec/tyv003 (suggesting that costs of attribution may actually decline with scale).

242. *See*, *e.g.*, Waxman, *supra* note 91, at 422 n.5; SHAKARIAN, SHAKARIAN & RUEF, *supra* note 169.

243. See Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 924–33 (1998) for an example of a discussion focused on

tractable hurdles to mapping traditional international law norms onto the cyber context, international law frameworks must shift toward such a dynamic analysis, which can draw on well-developed chaos theory. Acts of cyber warfare exhibit behavior closer in kind to that of weather than the conflicts public international law is premised upon, as David Brumley fittingly observed in referring to autonomous cyber weapons.[244]

CONCLUSION

As cyber warfare incidents become more frequent, forceful, and intricate, international law remains miles behind. Previous attempts to deal with the problem of cyber have failed to gain widespread state adoption because they do not properly account for the inherent differences between the cyber and traditional warfare contexts. Chaos theory, however, can be utilized effectively in developing a new international legal framework to address the complex and dynamic phenomena unique to cyber. From an art exhibit illustrating oceanic eddies to an Aegis operator's decision to run the technology using the fully automated doctrine, chaos theory has broad applicability to any dynamic system. To deal with keystrokes that can cause a total system and infrastructure halt across the world, legal frameworks must modernize to account for the features that make such consequences possible in the first place.

---

the risks of a use of force in response to a cyberattack, as opposed to the risk of incurring a cyberattack, which is more commonplace.

244. SCHARRE, *supra* note 70, at 217, 227.