ARTICLE

SWINGING A FIST IN CYBERSPACE

Jessica "Zhanna" Malekos Smith∗

I. INTRODUCTION

As the US Supreme Court Justice Oliver Wendell Holmes Jr. opined, "[t]he right to swing my fist ends where the other man's nose begins."[1] But when the force of a state's "fist" collides with another state's "nose," what rights are activated? Although the "use of force" is prohibited under Article 2(4) of the United Nations (UN) Charter,[2] two exceptions exist: (1) The collective security power of the UN Security Council; and (2) a state's inherent right

∗ Jessica "Zhanna" Malekos Smith, J.D. is a M.A. candidate with King's College London, Department of War Studies. Previously, she served as a Captain in the US Air Force Judge Advocate General's Corps. Prior to the military, Jessica was a Postdoctoral Fellow with the Belfer Center's Cyber Security Project at the Harvard Kennedy School. Opinions expressed in her articles are those of the author's and not those of the US Department of Defense or US Air Force. With special thanks to Thomas E. Smith and the diligent staff of the Houston Law Review for their generosity of time and support.

1. Annie Laurie Gaylor, *Oliver Wendell Holmes, Jr.,* FREEDOM FROM RELIGION FOUNDATION, https://ffrf.org/news/day/dayitems/item/14246-oliver-wendell-holmes-jr (last visited May 14, 2018).

2. NIGEL D. WHITE & CHRISTIAN HENDERSON, RESEARCH HANDBOOK ON INTERNATIONAL CONFLICT AND SECURITY LAW 118 (1996).

to self-defense under Article 51.

But how do these rights apply when a state swings its fist in cyberspace? Specifically, can Article 51 legitimately be used by states to justify the use of force against a malicious cyber operation? The central argument is that "cyber attacks" justify the invocation of Article 51 in the *jus ad bellum* ("right to war") as a defensive measure under international law; however, this is subject to limitations – the responding state's ability to credibly assess the scope and effects of the attack and attribute the attack source(s) and actor(s). Part II describes the relevant legal framework. Part III analyzes what constitutes a "cyber attack" and how context drives interpreting the scope and effects. Lastly, Part IV addresses the impediments to applying state responsibility in cyberspace.

II. LEGAL FRAMEWORK

Article 2(4) of the UN Charter prohibits the use of force and requires: "All members [to] refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state[.]"[3] Pursuant to the 1987 Declaration on the Non-Use of Force: "States have the inherent right of individual or collective self-defence if an armed attack occurs, as set forth in the Charter."[4] Specifically, Article 51 reads: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an **armed attack** occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."[5] To be clear, an "armed attack" in the *jus ad bellum* self-defense context is different from an "attack" in the *jus in bello* ("law in waging war"), international humanitarian law context. Although "armed attack" is a term of art, surprisingly, there is no uniform legal definition.[6] The United Kingdom's *Cyber Primer* explains that an armed attack "must be an act of armed force of sufficient gravity, having regard to its scale and effects."[7]

So how do states invoke their self-defense rights? Christine Gray explains "[i]n practice, states making their claims to self-de-

---

3. U.N. Charter, art. 2, para.4.

4. U.N. Declaration on Threat or Use of Force in International Relations, A/RES/42/22 (Nov. 18, 1987).

5. U.N. Charter, art. 51 (emphasis added).

6. UNITED KINGDOM MINISTRY OF DEFENCE, CYBER PRIMER 13 (2016) (emphasis added).

7. *Id.*

fence try to put forward arguments that will avoid doctrinal controversy and appeal to the widest possible range of states."[8] In 1986 the International Court of Justice (ICJ) ruled in *Nicaragua v. United States* that if a member state exercises its inherent right to individual self-defense, the state must have been a victim of an armed attack.[9]

While the Court did not define "armed attack," it described the general nature as "acts which can be treated as constituting armed attacks."[10] Specifically, "if such an operation, **because of its scale and effects**, would have been classified as an armed attack rather than as a mere frontier incident, had it been carried out by regular armed forces."[11] Thus, the scale and effects of an operation are requisite inputs for evaluating an armed attack, which in turn provides the state's legal justification for invoking Article 51.

III. DEFINING CYBER ATTACKS

Under Rule 30 of the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, a cyber attack is a "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[12] Although no standard international legal definition exists, that is not the problem; according to Dr. Michael Sulmeyer of the Harvard Kennedy School's Cyber Security Project, "[t]he problem is not the lack of definitions, but a lack of consensus about what bad conduct in cyberspace really needs to be stopped."[13] More recently, in a June 2018 address at the National Security Agency, US Senator Mark Warner (D-VA) bemoaned the lack of clarity on what cyber activities are tantamount to an attack and warned that '[f]ailing to articulate a clear policy and to set expectations about when and where we will respond to cyber-attacks, is not just bad policy. It is downright dangerous.'[14]

To that issue, what "bad conduct" in cyberspace legitimately rises to the level of an "armed attack"? International legal scholar,

---

8. CHRISTINE D. GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 118 (2008).
9. Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 195 (June 27).
10. *Id.*
11. *Id.* (emphasis added).
12. MICHAEL N. SCHMITT, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 106 (2013).
13. Michael Sulmeyer, *Which Cyberattacks Should the US Deter, and How Should it be Done?*, COUNCIL ON FOREIGN RELATIONS, https://www.cfr.org/blog/which-cyberattacks-should-united-states-deter-and-how-should-it-be-done (last visited May 14, 2018).
14 Mark Warner, *2018 NSA Law Day Speech,* LAWFARE, https://www.lawfare-blog.com/2018-nsa-law-day-speech (last visited June 13, 2018).

Yoram Dinstein, offers several examples: "Fatalities caused by the loss of computer-controlled life-support systems; an extensive power grid outage (electricity blackout) creating considerable deleterious repercussions; a shutdown of computers controlling waterworks and dams, generating thereby floods of inhabited areas; deadly crashes deliberately engineered (e.g., through misinformation fed into aircraft computers)" and "the wanton instigation of a core-meltdown of a reactor in a nuclear power plant, leading to the release of radioactive materials that can result in countless casualties if the neighbouring areas are densely populated."[15]

What do these examples share in common? They only reference kinetic effects. Some "attacks," however, do not produce physical destruction, but harm only data and data systems. This disjunction between discerning harm in the cyber and kinetic sphere is referred to as the "cyber boundary."[16] This boundary is "the decision point when a commander must decide whether and how to move from a purely cyber war to one involving conventional forces, or kinetic weapons. Crossing the boundary is an escalatory step that may lead to war spiraling out of control."[17]

Although it is unclear if the scope of armed attacks will be broadened, the US is leveraging the term protected "critical infrastructure" to expand this area of impermissible attack vectors. In 2017, the US Department of Homeland Security designated election infrastructure, (i.e. data systems) as "critical infrastructure."[18] The 2001 Patriot Act defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security[.]"[19]

From the United Kingdom Ministry of Defense's perspective, "[a] cyber operation may constitute an armed attack if its method, gravity and intensity of force is such that its effects are equivalent to those achieved by a kinetic attack which would reach the level of an armed attack."[20] The general international consensus is that the scope and effects of the cyber operation shape the victim state's characterization of it.[21] By examining the severity of these facets,

---

15. MARCO ROSCINI, WORD WIDE WARFARE: JUS AD BELLUM AND THE USE OF CYBER FORCE 115 (2010).

16. RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR 283 (2010).

17. RK TYAGI, UNDERSTANDING CYBER WARFARE AND ITS IMPLICATIONS FOR INDIAN ARMED FORCES, at vii (2013).

18. Jeh Johnson, *Designation of Election Infrastructure*, U.S. DEP'T OF HOMELAND SECURITY, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical (last visited May 14, 2018).

19. 42 U.S.C. § 519c(e) (2012).

20. *Id.*

21. MICHAEL N. SCHMITT, COMPUTER NETWORK ATTACKS AND THE USE OF FORCE IN

states evaluate whether the operation meets the requisite threshold of an armed attack.

IV. STATE RESPONSIBILITY

If a state suffered a debilitating cyber attack on its national banking system and invoked Article 51 as a defensive measure, would it matter if the attack emanated from a state, or non-state actor? In a word, yes. The 2018 US Department of Defense's National Defense Strategy Summary makes clear that "[s]tates are the principal actors on the global stage, but *non-state actors* also threaten the security environment with increasingly sophisticated capabilities. Terrorists, trans-national criminal organizations, cyber hackers and other malicious non-state actors have transformed global affairs with increased capabilities of mass disruption."[22]

Ultimately, the legal analysis hinges on state responsibility. The *Tallinn Manual* provides a framework for norm-building here: "States bear responsibility for an act when: (i) the act in question is attributable to the State under international law; and (ii) it constitutes a breach of an international legal obligation applicable to the States[.]"[23] The ICJ's approach has been to evaluate whether an "armed attack" waged by non-state actors can be imputed to the state.[24] In *Nicaragua*, the Court evaluated whether the US' actions in supporting the *contras* were imputable to the state, such that the US "had effective control of the military or paramilitary operation[.]"[25]

Thus, if a state has effective control over the cyber operation waged by the non-state actor, responsibility could be imputed.

Although determining the attack origin and actor(s) is significant, just war ethics and international law struggle with attribution. According to Matthew Waxman, the complexities of attribution stem from "the technical aspects and the ability to make those findings public in a credible, persuasive way, as well as the secrecy and low visibility of some states' responsive actions in cyberspace[.]"[26] Putting it all together, if the operation constitutes an "armed attack" and is credibly attributed to a state, or non-state

---

INTERNATIONAL LAW 4 (2012).

22. U.S. DEPT. OF DEFENSE, SUMMARY OF THE 2018 NATIONAL DEFENSE STRATEGY OF THE US OF AMERICA 3 (2018).

23. SCHMITT, *supra* note 12, at 29.

24. Nicaragua, *supra* note 9, at 115.

25. *Id*.

26. MATTHEW A. WAXMAN, CYBER ATTACKS AND THE USE OF FORCE: BACK TO THE FUTURE OF ARTICLE 2(4) 445 (2011).

group with sufficient ties to impute state responsibility, the victim state's invocation of individual self-defense is legally justifiable. This assumes, however, that attribution can be achieved in a timely, accurate and cost-effective manner. Simply put, the victim state must assess – is the juice worth the squeeze? Lastly, the victim state's response must be measured to satisfy the legal principles of necessity and proportionality.[27]

V. CONCLUSION

Regardless of the medium in which conflict is waged, Livy's observation holds true: "There are laws of war as well of peace;"[28] Thus, when a state swings its fist in cyberspace it also takes an emboldened step into the arena of conflict. And the effects of entering this "colosseum" are just as keenly felt as that of the blade of a gladiator's sword. As this essay has explained, when the force of a state's "fist" collides with another state's "nose," certain legal rights are triggered. Here, states can legitimately invoke Article 51 to justify the use of force against cyber attacks; however, whenever a state invokes this inherent right of self-defense, they act at their own discretion and risk in following these principles.[29]

---

27. SCHMITT, *supra* note 20, at 4.

28 TITUS LIVIUS (LIVY), THE HISTORY OF ROME, Book V, Chapter 27, line 7, *also available at:* http://www.perseus.tufts.edu/hopper/text?doc=Perseus%3Atext%3A1999.02.0145%3Abook%3D5%3Achapter%3D27 (last visited June 14, 2018).

29. YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 187(2011).