

2021

## Self-Defense to Cyber Force: Combatting the Notion of 'Scale And Effect'

Thomas Eaton

Follow this and additional works at: <https://digitalcommons.wcl.american.edu/auilr>



Part of the [Internet Law Commons](#)

---

### Recommended Citation

Eaton, Thomas (2021) "Self-Defense to Cyber Force: Combatting the Notion of 'Scale And Effect'," *American University International Law Review*. Vol. 36 : Iss. 4 , Article 1.  
Available at: <https://digitalcommons.wcl.american.edu/auilr/vol36/iss4/1>

This Article is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in American University International Law Review by an authorized editor of Digital Commons @ American University Washington College of Law. For more information, please contact [kclay@wcl.american.edu](mailto:kclay@wcl.american.edu).

**SELF-DEFENSE TO CYBER FORCE:  
COMBATting THE NOTION OF ‘SCALE AND  
EFFECT’**

THOMAS EATON\*

I. INTRODUCTION .....697

II. WHY THIS QUESTION IS IMPORTANT..... 702

III. STARTING WITH THE TEXT ..... 704

IV. CHARTER-IS-DEAD SCHOOL ..... 706

V. SCALE AND EFFECTS SCHOOL ..... 710

VI. PROBLEMS WITH SCALE AND EFFECTS SCHOOL.715

    A. PREDICTIVE PROBLEMS..... 717

    B. DESCRIPTIVE PROBLEMS. .... 719

        i. Problems with Scale and Effects, as conceived..... 720

        ii. Problems with Scale and Effects, as applied ..... 727

VII. HOW TO BETTER THINK ABOUT SCALE AND  
EFFECTS OF CYBER OPERATIONS. .... 730

VIII. PRESCRIPTIVE PROBLEMS..... 742

IX. FORCEFUL COUNTERMEASURES SCHOOL ..... 745

X. NO GAP SCHOOL ..... 754

XI. CONCLUSION ..... 768

**I. INTRODUCTION**

In early December, it was announced that United States (U.S.) companies SolarWind and FireEye were the victims of a widespread

---

\* The author is a Judge Advocate in the United States Navy. The views expressed in this writing are the author’s alone and do not represent the views of the Department of the Navy or the United States Government. The author would like to thank Breawna Power Eaton, for reading numerous drafts, providing excellent feedback, and always being his best editor—both professionally and personally. The author would also like to thank the Editorial Staff at the American University International Law Review for vastly improving this writing, and importantly the faculty of The Fletcher School, particularly, Professors Tom Dannenbaum and Michael Glennon.

and pervasive cyber-attack that possibly affected tens of thousands of government computers. “[T]he magnitude of this ongoing attack is hard to overstate.”<sup>1</sup> While the attack remains under investigation at the time of this writing, “[e]vidence in the SolarWinds attack points to the Russian intelligence agency known as the S.V.R., whose tradecraft is among the most advanced in the world.”<sup>2</sup> What will happen next, with regard to both how the U.S. will respond and what they can and will do to prevent future attacks, remains uncertain.

A major reason for this uncertainty is that the entire spectrum of cyber warfare challenges the paradigm of how “war” has been traditionally defined. The right to self-defense is present in almost all legal systems, both between persons and between states. Between nations, the debate over what level of force justifies a lawful use of force in response, purportedly laid out in the United Nations Charter, began even before the Charter was signed. Defining force in the cyber domain poses new challenges, yet this unique, quickly evolving facet of warfare has simply been pasted on top of the older, unresolved debate.

It would be overly ambitious to attempt to resolve fundamental, long-debated disagreements about how to read the language of Arts. 2(4) and 51. However, the analysis applied by the majority view – looking at the “scale and effect” of cyber operations, as in Tallinn Manual 2.0 – is unrealistic, unworkable, and undesirable. The challenge of defining force in the cyber domain remains; however, descriptively, predictively, and proscriptively, states are justified in responding to *any* force with counterforce in self-defense, proportionality acts as the throttle to self-defense, rather than the unreasonably high standard of “scale and effect.”

The ability to reach out, with a few keystrokes or a couple lines of code, through the interconnected world of cyberspace and create militarily advantageous effects 10,000 miles away has changed warfare as previously conceived, perhaps more than any other

---

1. Thomas P. Bossert, Opinion, *I Was the Homeland Security Adviser to Trump. We're Being Hacked*, N.Y. TIMES (Dec. 16, 2020), <https://www.nytimes.com/2020/12/16/opinion/fireeye-solarwinds-russia-hack.html>.

2. *Id.*

advancement in any other domain of war. Cyber weapons are weapons, and whatever law applies to conventional weapons equally applies to cyber weapons.<sup>3</sup> Long before cyber operations were even science fiction, there was much debate over what constituted a use of force that would justify force in response. In many ways, the debate over what constitutes cyber-attacks has been pasted on top of that older debate, but the unique form of harm that cyber-attacks cause adds novel questions to these older debates. Lacking a physical instrument, yet possessing the potential to cause greater harm, cyber-attacks seem simultaneously less and more “forceful.” How one views that dichotomy, coupled with how they generally view the Charter regarding conventional force, has led to varying answers to the salient question: what is the threshold of cyber force required to justify the use of counterforce in self-defense?

When something breaks on the receiving end of a cyber-attack—when people die, when fires erupt, when opened dams destroy villages—few seem to disagree<sup>4</sup> the act would be a “use of force,” likely rising to the level of an “armed attack” that would justify lawful force in “self-defense” in response, regardless how one regards the text of Article 51 of the United Nations (UN) Charter.<sup>5</sup> The far more complicated question is: what happens when nothing “physical” breaks? When only data is destroyed, when government email stops working, when banking systems fail, when stock markets crash, but no one is injured, no property is destroyed?

A cyber-attack is not “a monolithic technique . . . there are many methods by which computer networks have been, or could be, attacked.”<sup>6</sup> Each attack must be analyzed individually. However, the most widely accepted view, as advanced in the Tallinn Manual 2.0,

---

3. See Daniel B. Silver, *Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter*, 76 INT’L L. STUD. SERIES U.S. NAVAL WAR COLL. 73, 76 (2002) (noting that using a weapon to target a computer raises the same questions under international law as would the targeting of any other piece of equipment).

4. See TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 341 (Michael N. Schmitt ed., 2nd ed. 2017) [hereinafter TALLINN MANUAL 2.0].

5. See U.N. Charter arts. 2, ¶ 4, 51.

6. Silver, *supra* note 3, at 76 (proceeding to discuss various means of cyber-attacks).

looks to the “scale and effects”<sup>7</sup> test adopted from the International Court of Justice’s (ICJ) judgment in the *Military and Paramilitary Activities in and Against Nicaragua*.<sup>8</sup> This classic analysis is reasonable at first glance, if one accepts a textual reading of the UN Charter, even with limited modification based on subsequent state practice and judicial decisions, as did the authors of the Manual (the self-proclaimed International Group of Experts (IGEs)).<sup>9</sup> Others have argued that state practice has irretrievably broken the language of the Charter, asserting that even engaging in a discussion over how to interpret the terms “armed attack” in differentiation of “use of force” is meaningless—states will do what states do.<sup>10</sup>

Various framings and weights given to the varying sources of authority of how to interpret the language of the Charter, subsequent state practice, and judicial decisions place the starting point of this analysis in vastly different locations. Sean Murphy offers “Four Schools of Thought” on how to interpret the UN Charter on the question of preemptive self-defense.<sup>11</sup> His Schools on that question are: “‘The Strict-Constructionist School,’ ‘The Imminent Threat School,’ ‘The Qualitative Threat,’ and ‘The ‘Charter-Is-Dead’ School.’”<sup>12</sup>

---

7. See TALLINN MANUAL 2.0, *supra* note 4, at 330–31 (referring to “scale and effects” as “a shorthand term that captures the quantitative and qualitative factors to be analyzed in determining whether a cyber operation amounts to the use of force”).

8. See *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 195 (June 27).

9. See TALLINN MANUAL 2.0, *supra* note 4.

10. See, e.g., Michael J. Glennon, *What’s Law Got to Do with It?*, 26 WILSON Q. 70, 75 (2002) (arguing that states act alone when acting multilaterally is not in their best interest); Thomas M. Franck, *Who Killed Article 2(4)? Or: Changing Norms Governing the Use of Force by States*, 64 AM. J. INT’L L. 809, 809 (1970) (acknowledging that historically, states have sometimes “succumbed to the temptation to settle a score, to end a dispute or to pursue their national interest through the use of force”). But see W. Michael Reisman, *Thomas Franck and the Use of Force*, 104 AM. SOC’Y INT’L L. PROC. 403, 406 (2010) (highlighting the United Nations’ major contribution of prohibiting war as individual state policy, instead replacing it with a collective security system).

11. See Sean D. Murphy, *The Doctrine of Preemptive Self-Defense*, 50 VILL. L. REV. 699, 706 (2005) (acknowledging that the ‘Schools’ rest upon broad conceptions of international law and that international lawyers within a specific school may differ in certain respects).

12. *Id.* at 706–19.

Murphy was analyzing a different question, but his schools offer four general views on the status of the language of the Charter.<sup>13</sup> Adapting the labelling of his four Schools to reflect the current question – how to define the threshold of a use of force justifying self-defense – I offer: The ‘Charter-Is-Dead’ School, The Scale and Effects School, The Forceful Countermeasures School, and The No Gap School. How one approaches the language in Articles 2(4) and 51, generally, and the weight given to sources of interpretation, likely lead to how one views the more specific and novel questions of force regarding cyber operations.<sup>14</sup>

Briefly, the Charter-Is-Dead School is clearly the outlier, which would hold, as the name implies, that the language of the Charter is dead, and states are lawfully free to use force at any time.<sup>15</sup> However, the Scale and Effects School, when applied to conventional and cyber warfare, is most problematic in both its logic and widespread acceptance.<sup>16</sup> The problems begin with the theory’s establishment of an unreasonably high threshold for the “most grave”<sup>17</sup> uses of force required to constitute an “armed attack” that would justify “self-defense,” and these problems become all the more obvious in the cyber domain.<sup>18</sup> The Forceful Countermeasures School creates a messy, complicated explanation that does provide more realistic remedies for victims of force, but finds very little support in the text or *claimed* practice.<sup>19</sup> A focus on cyber operations demonstrates that The No Gap School provides the best predictive (what states will do), descriptive (what the law is), and prescriptive (what the law should be) analysis.<sup>20</sup> Ultimately, much consensus building still must be done. In 2002,

---

13. *See id.*

14. *See generally* 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, 426–40 (2011) (exploring the various interpretations of Articles 2(4) and 51).

15. *Infra* Part IX; *see also* Murphy, *supra* note 11, at 717–18 (introducing the Charter-Is-Dead School).

16. *Infra* Part IX; *see also* Murphy, *supra* note 11, at 706–11 (what Murphy referred to as the ‘Strict-Constructionist’ School).

17. Murphy, *supra* note 11, at 709–10; *see also* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 191 (June 27).

18. *See* U.N. Charter art. 51.

19. *Infra* Part IX.

20. *Infra* Part IX.

Daniel Silver believed, “[i]t is too early for any legal authority to emerge on the status of [cyber-attacks] under Article 2(4).”<sup>21</sup> Almost two decades have passed, and the Scale and Effects School and Tallinn Manual claims to be that legal authority.<sup>22</sup> State practice, however, proves that consensus false, nor is “scale and effect” prescriptively what the law should be.<sup>23</sup>

## II. WHY THIS QUESTION IS IMPORTANT.

To begin with the obvious, the internet powers our modern lives. The “digital economy” alone consists of 6.9% of total U.S. GDP, and “Information Technology” makes up 19.9% of the value of Standard and Poor’s 500 (S&P).<sup>24</sup> But it is hard to imagine the scale of potential damage to other sectors that a large-scale cyber-attack could cause, such as the Financial Sector, adding 20.7% to GDP, or just “Financials” (13.7%) and “Communication Services” (9.9%) of the S&P.<sup>25</sup> Literally trillions of dollars, the proverbial wealth of nations. Consider this: Cash only makes up 33% of current payments in the U.S.<sup>26</sup> While higher in some countries (78.8% in Europe), cash remains the dominant method of payment across the world; however, there is a general trend of moving away from cash transactions.<sup>27</sup> The ability

21. Silver, *supra* note 3, at 75.

22. See Michael N. Schmitt, *The Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't*, JUST SEC. (Feb. 9, 2017), <https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/> (introducing the Tallinn Manual).

23. *Infra* Part IX.

24. *Digital Economy Accounted for 6.9 Percent of GDP in 2017*, NAT'L TELECOMMS. & INFO. ADMIN. (Apr. 5, 2019), <https://www.ntia.doc.gov/blog/2019/digital-economy-accounted-69-percent-gdp-2017> [hereinafter *Digital Economy*]; Tim Lemke, *What is the Weighting of the S&P 500?*, BALANCE, (Dec. 22, 2020), <https://www.thebalance.com/what-is-the-sector-weighting-of-the-s-and-p-500-4579847>.

25. See *Digital Economy*, *supra* note 24; Lemke, *supra* note 24.

26. RAYNIL KUMAR ET AL., FED. RSRV. SYS., 2018 FINDINGS FROM THE DIARY OF CONSUMER PAYMENT CHOICE 3, 10 (Nov. 1, 2018), <https://www.frbsf.org/cash/files/federal-reserve-cpo-2018-diary-of-consumer-payment-choice-110118.pdf>.

27. See G4S, WORLD CASH REPORT 2018 25 (2018), <https://www.g4scashreport.com/> (assessing the position of cash for transactional purposes); CAPGEMINI, WORLD PAYMENTS REPORT 2019 32–35 (2019), <https://www.capgemini.com/es-es/wp-content/uploads/sites/16/2019/09/World->

to stop or even somewhat slow non-cash transactions would cripple economic systems, and thereby debilitate the national structure of government.<sup>28</sup>

The 2007 “botnet” attack against Estonia, demonstrated the power of cyber operations: “This was not the first botnet strike ever, nor was it the largest. But never before had an entire country been targeted on almost every digital front all at once.”<sup>29</sup> For weeks, “cash machines and online banking services were sporadically out of action; government employees were unable to communicate with each other on email; and newspapers and broadcasters suddenly found they couldn’t deliver the news,” effectively crippling Estonia.<sup>30</sup> The attacks were popularly attributed to Russia, over a dispute centering the removal of a Soviet era World War II memorial.<sup>31</sup> However, the use of “zombies” – “computers from around the world that had been hijacked previously by hackers” – as well as specialized “hackers who could infiltrate individual Web sites, delete legitimate content, and post their own messages,” while routing through third countries such as Egypt, Vietnam, and Peru, attempted to obfuscate the operation’s true origins.<sup>32</sup> Attribution of responsibility to any particular state of any cyber operation will always be the fundamental challenging factual and legal question.<sup>33</sup> For the purpose of this writing, that fundamental question will be put aside as a factual matter, and state direction with requisite control to find state responsibility will be assumed.<sup>34</sup> Attacks

---

Payments-Report-WPR-2019.pdf (detailing the growth of non-cash transactions).

28. See CAPGEMINI, *supra* note 27, at 32–35.

29. Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007), <https://www.wired.com/2007/08/ff-estonia/> (emphasizing that this was the first time ever that a botnet threatened an entire nation’s national security).

30. Damien McGuinness, *How a Cyber Attack Transformed Estonia*, BBC NEWS (Apr. 27, 2007), <https://www.bbc.com/news/39655415>.

31. See Davis, *supra* note 29.

32. *Id.* (concerning the challenges of cyber attribution); see also Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 INT’L L. STUD. SERIES U.S. NAVAL WAR COLL. 99, 107 (2002) (“The trouble, however, is that frequently the server which is seemingly the source of the [cyber-attack] has only been manipulated by the true assailants”).

33. See Silver, *supra* note 3, at 78 (noting that the issue of attributability “is exacerbated by the amorphous structure of the Internet”).

34. See *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶¶ 115, 121 (June 27) (“effective control”);



like Estonia's debilitating disruption will not be an enigma, neither will they simply become more prevalent: they are the future of warfare.<sup>35</sup>

### III. STARTING WITH THE TEXT

At first glance, the drafters of the UN Charter laid out a rather straightforward approach to the use of force in Article 2(4): "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state. . . ."<sup>36</sup> The text leaves open two possible exceptions to this general prohibition, and both have elicited substantial debate over interpretation.<sup>37</sup>

First, the Security Council itself may authorize the use of force by finding, in accordance with Article 39, "the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore *international* peace and security."<sup>38</sup> Then, in Article 41, "[t]he Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions. . . ."<sup>39</sup> Then, in Article 42, "[s]hould the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security."<sup>40</sup>

---

Prosecutor v. Tadić, Case. No. IT-94-1-A, Judgment, ¶ 120 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999) ("overall control"). Discussing issues of what would constitute responsibility are, again, beyond the scope of this writing; for the purpose of this writing state responsibility, at whatever the requisite level is assumed.

35. See Davis, *supra* note 29 (comparing the advent of information warfare with the advent of nuclear technology).

36. U.N. Charter art. 2, ¶ 4.

37. See U.N. Charter arts. 39, 41–42. There is a possibility that consent of the state affected. For this writing and analysis, the assumption is that the effects of a cyber operation are non-consensual.

38. U.N. Charter art. 39 (emphasis added).

39. U.N. Charter art. 41.

40. U.N. Charter art. 42. The drafters envisioned a (never materialized) standing force, comprised of forces contributed by member states, to be employed by the

The debate over Security Council sanctioned uses of force surround when (if ever) the Security Council can, in what Article 2(7) purports to prohibit, “intervene in matters which are essentially within the domestic jurisdiction of any state.”<sup>41</sup> Also, how to interpret the terms “threat to the peace, breach of the peace, or act of aggression,” in light of the term “international peace” in the last phrase.<sup>42</sup> Does the term “international” modify the entire article, effectively limiting the Security Council’s scope, together with Article 2(7), to only matters of cross-border violence, or is a threat to peace (international or otherwise) whatever the Security Council says it is?

The International Court of Justice potentially has the power to clarify the scope of the Security Council’s discretion, as “[t]he Court has not hesitated to tell other organs of the United Nations that they may not exceed their assigned powers.”<sup>43</sup> The court having “never [ . . . ] declared any act of the Security Council invalid as beyond the scope of its authority,” “sees thus far to have left open the question. . . .”<sup>44</sup> Professor Glennon’s *textual* conclusion is that Articles 39 and 2(7) read together limit Security Council action to “at least a threat of action by a state that is (a) violent and (b) has cross-border effects.”<sup>45</sup> The Security Council has generally followed this restriction, but beginning in 1966 with Rhodesia, “cracks began to appear in the old anti-interventionist regime.”<sup>46</sup> Especially between the five Permanent Members, politics, not the text, is clearly the best predictor of when the Security Council will and will not take action, particularly when dealing with what could be viewed as “within the domestic jurisdiction”<sup>47</sup> of a state.<sup>48</sup> This debate need not be resolved

---

Security Council in Art. 43.

41. U.N. Charter art. 2, ¶ 7.

42. U.N. Charter art. 39.

43. MICHAEL J. GLENNON, *LIMITS OF LAW, PREROGATIVES OF POWER: INTERVENTIONISM AFTER KOSOVO* 103 (2001) [hereinafter *INTERVENTIONISM AFTER KOSOVO*].

44. *Id.*

45. *Id.* at 108.

46. *Id.* at 113.

47. U.N. Charter art. 2, ¶ 7.

48. See generally Frederic L. Kirgis, Jr., *The Security Council’s First Fifty Years*, 89 AM. J. INT’L L. 506 (1995) (exploring the Security Council’s changes throughout its first fifty years of existence).

for the purposes of this writing, since I will only be considering cyber operations that are cross-border, state-on-state actions, the dominant, yet still “unworkable”<sup>49</sup> system, wherein the Security Council has chosen to intervene, though they might be considered internal affairs.

The second exception for the lawful use of force, and the subject of this writing, Article 51, permits states to use force “until” (perhaps, before) the Security Council acts in “individual or collective self-defense if an armed attack occurs against a member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security.”<sup>50</sup>

Far more debate has ensued over Article 51. The question of preemptive self-defense is perhaps the dominant issue, addressed by Murphy’s original four Schools, because the Security Council rarely acts and states usually claim to be using force in self-defense when they do.<sup>51</sup> Adherents of the four schools, along different lines, diverge over the threshold, interpretive question about the weight to give text, legal opinions, and state practice.<sup>52</sup> The three main questions of law on which the schools differ are as follows: 1) is there a difference between the terms “use of force” and “armed attack?” 2) if so, what is the practical “gap” between the two? and 3) again, if there is a difference, what action is authorized within that gap? No school asserts that cyber violence cannot be force, but it is necessary to answer these questions regarding conventional force, in order to project how each School views the questions in the cyber domain.

#### IV. CHARTER-IS-DEAD SCHOOL

The group most likely to find the forgoing discussion meaningless and overly tedious would be the Charter-Is-Dead School, which holds that “the prohibition against the use of force in relations between states has been eroded beyond recognition.”<sup>53</sup> The Charter-Is-Dead School

---

49. John Lawrence Hargrove, *The Nicaragua Judgment and the Future of the Law of Force and Self-Defense*, 81 AM. J. INT’L L. 135, 136 (1987) (“internationally authorized military coercion has proven unworkable”).

50. U.N. Charter art. 51.

51. Murphy, *supra* note 11, at 699 (analyzing the doctrine of preemptive self-defense).

52. *See id.*

53. Franck, *supra* note 10, at 835. *But see* TALLINN MANUAL 2.0, *supra* note 4,

would argue that whatever the original meaning and intent of the drafters on the interplay between Articles 2(4) and 51, subsequent state practice has eviscerated any remaining meaning.<sup>54</sup> “The practice of these states has so severely shattered the mutual confidence which would have been the *sine qua non* of an operative rule of law embodying the precepts of Article 2(4) that . . . only the words remain.”<sup>55</sup> Prof. Glennon writes, “the Charter provisions governing the use of force are simply no longer regarded as binding international law.”<sup>56</sup>

Various scholars, sampling from various time periods, record the sheer quantity of post Charter armed conflict:<sup>57</sup> “Between 1945 and 1980, there were over 100 wars;”<sup>58</sup> “some 90 armed conflicts between 1989 and 1993;”<sup>59</sup> “in February 1998 . . . 30 ‘major ongoing wars;”<sup>60</sup> and, as of 2018, “at least 69 armed conflicts occurred on the territory of 30 states.”<sup>61</sup> Glennon continues, “not all war necessarily involves a use of force in violation of Article 2(4) . . . [but, t]ruly international conflict[s], however, *would* necessarily entail an unlawful use of force inasmuch as not every participant can avail itself of the self-defense exception.”<sup>62</sup> States as lawmakers in the international positivist system are “bound only by rules to which they consent. A treaty can lose its binding effect if a sufficient number of parties engage in conduct that

---

at 330 (discussing “scale and effects” as a measure of determining whether a particular action constitutes an armed attack).

54. See Murphy, *supra* note 11, at 717–19 (“the rules have fallen into desuetude”).

55. Franck, *supra* note 10, at 809.

56. Michael J. Glennon, Opinion, *How War Left Law Behind*, N.Y. TIMES, (Nov. 21, 2002), <https://www.nytimes.com/2002/11/21/opinion/how-war-left-the-law-behind.html> [*hereinafter How War Left Law Behind*]; see also INTERVENTIONISM AFTER KOSOVO, *supra* note 43, at 85–86.

57. *Id.* at 67–69.

58. *Id.* at 67.

59. *Id.* at 68 (citing Peter Wallensteen and Karin Axell, *Conflict Resolution and the End of the Cold War 1989-1993*, 31 J. PEACE RES. 333 (1994)).

60. *Id.* at 69 (citing THE CARTER CENTER, CONFLICT RESOLUTION UPDATE: UPDATE ON WORLD CONFLICTS (1998)).

61. ANNYSSA BELLAL, GENEVA ACAD., THE WAR REPORT: ARMED CONFLICTS IN 2018 19 (Apr. 2019), <http://www.rulac.org/news/the-war-report-armed-conflicts-in-2018>.

62. INTERVENTIONISM AFTER KOSOVO, *supra* note 43, at 69.

is at odds with the constraints of the treaty.”<sup>63</sup> The irony is that “[p]olicy makers are of course loath to admit th[is].”<sup>64</sup>

The Charter-Is-Dead School would not necessarily argue that states resort to violence with the frequency of a Hamilton duel, but that power, particularly the *relative* power of states, will be the governing force on states, not the text of the Charter.<sup>65</sup> For the Charter-Is-Dead School, if state practice has eviscerated the law against the use of force, then a differentiation between words like “use of force” versus “armed attack,” versus “scale and effect,” and “most grave” versus a “mere frontier incident” lacks any meaning.<sup>66</sup> If there is no longer (or never was) a prohibition on the use of force, it is unhelpful to analyze when, if ever, to classify a cyber operation as such.<sup>67</sup>

The School would view cyber-attacks the same way Glennon analyzed support for terrorism: “If there is no authoritative general prohibition of the use of force, it makes no sense to consider the breadth of a possible exception.”<sup>68</sup> Looking at the 2007 cyber-attacks in Estonia, the Charter-Is-Dead argument would follow that Estonia did not respond to Russia’s attack, not because they viewed the operation as not rising to the level of the scale and effect of an armed attack, but because responding with force, cyber or physical, would ignite a war Estonia would surely lose.<sup>69</sup> Conversely, if the alleged perpetrator and target were reversed, Russia would not restrain itself simply because the attack did not cross the gravity threshold to allow self-defense.<sup>70</sup> Russia would likely respond with force, if it viewed doing so to be in its best interest—the law be damned.<sup>71</sup> The varying

---

63. *How War Left Law Behind*, *supra* note 56.

64. *Id.*

65. INTERVENTIONISM AFTER KOSOVO, *supra* note 43, at 2–3 (arguing that no rule has successfully obliged states to refrain from intervention).

66. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶¶ 191, 195 (June 27).

67. See 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, 541 (2002).

68. *Id.*

69. ALISON LAWLOR RUSSELL, CYBER BLOCKADES 69, 88 (2014) (noting that Estonia ultimately classified the cyber-attacks as criminal activity).

70. *Id.* at 131.

71. *Id.* at 87.

applications of the debated principle of desuetude differentiates scholars based on the degree to which they view the rule against the use of force in Article 2(4) has been changed by custom.<sup>72</sup> But all adherents would assert that functionally, “[t]he United Nations Charter today bears little more resemblance to the modern world than does a Magellan map.”<sup>73</sup>

The Charter-is-Dead School appears to have significant expository and predictive power.<sup>74</sup> Looking back to why states did or did not use force as well as looking forward and hypothesizing when states will use force, power, and national interest seems far more salient than law.<sup>75</sup> “Critics may argue that states involved in conflict will always put their vital interests first.”<sup>76</sup> Finally, descriptively (as to what the law is), no one believes that the UN Charter system is working well, and the Charter-is-Dead School makes the most honest attempt to deal with how to treat the widespread, Charter-violating, state practice of use of force.<sup>77</sup>

While the Charter-is-Dead School seems to get closest to a unified theory explaining state practice, it seems unhelpful to stop here and declare there is no prohibition against the use of conventional or cyber force.<sup>78</sup> Certainly, though actions loudly speak otherwise, not all states believe this position. In powerful states (U.S., Russia, China), future *personal* criminal liability for international crimes is unlikely;<sup>79</sup>

---

72. See INTERVENTIONISM AFTER KOSOVO, *supra* note 43, at 60–61 (“The concept of desuetude describes the process by which subsequent custom or practice supplants a treaty norm . . . Hans Kelsen considered desuetude the ‘negative legal effect of custom’ . . . if [a] written instrument derived force by virtue of public acceptance, inconsistent custom must be given effect by the same practice. Still, the concept of desuetude is controversial . . . [c]ustom inconsistent with a treaty constitutes, at least initially, a violation of the treaty.”).

73. Franck, *supra* note 10, at 810.

74. Dinstein, *supra* note 32, at 108.

75. Hargrove, *supra* note 49, at 136–37.

76. *Documents on the Laws of War* 15 (Adam Robert & Richard Guelff eds., 1982).

77. See TALLINN MANUAL 2.0, *supra* note 4, at 352.

78. See David Kretzmer, *The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum*, 24 EUR. J. INT’L L. 235, 246 (2013).

79. David Davenport, *Will the International Criminal Court Prosecute Americans Over Afghanistan?*, FORBES (Mar. 26, 2018), <https://www.forbes.com/sites/daviddavenport/2018/03/26/will-the-international->

however, many partner nations of the U.S., (i.e. NATO nations) have domestic law liability for international crimes.<sup>80</sup> While the Charter-is-Dead may be right that power and national interest are the most important factors in determining state action, they go too far in claiming that law has zero impact on decision makers.<sup>81</sup> Neither should we want power to be the *only* thing that has the force of law, especially since what humans might view as law is a complicated mix of what is actually enforceable, what we believe to it be, as well as a small sprinkling of what we might wish it to be. In powerful states, the effect of legitimating the Charter's force may be tertiary at best, but this will vary country to country.<sup>82</sup> Assuming, as the Charter-is-Dead School does, that state practice has fully eroded the language of Articles 2(4) and 51, it is still curious that states rarely admit to unsanctioned force, yet use conventional legal arguments to explain their actions as lawful; thus, even assuming its potential lowest ebb, law still has some bearing on how states justify their actions.<sup>83</sup>

## V. SCALE AND EFFECTS SCHOOL

The Tallinn Manual adopts the “scale and effects” test from the *Nicaragua* judgment in what can only be described as the most classic approach to interpreting the UN Charter, which is entirely appropriate and predictable.<sup>84</sup> After all, the Tallinn Manual 2.0 is— “[t]he product of a four-year follow-on project by a new group of 19 renowned international law experts [self-styled as the International Group of Experts, or the IGE] . . . the project benefited from the unofficial input of many states and over 50 peer reviewers.”<sup>85</sup> Albeit with some

---

criminal-court-prosecute-americans-over-afghanistan/#314f736010a5.

80. See generally Cleo Meinicke, *Domestic Prosecution of International Crimes – Introduction*, PILPG (March 7, 2019), <https://www.publicinternationallawandpolicygroup.org> (exploring some of the principles under which domestic laws may be used to prosecute international crimes).

81. See TALLINN MANUAL 2.0, *supra* note 4, at 334.

82. See 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, 586 (2018).

83. See TALLINN MANUAL 2.0, *supra* note 4, at 346.

84. See *id.* at 331, 334; see also Kretzmer, *supra* note 78, at 263.

85. TALLINN MANUAL 2.0, *supra* note 4, at intro.

internal disagreement at where to draw the line, the thread tying the Scale and Effect School together is a differentiation between what adherents would describe as the lower level of violence term “use of force” from Article 2(4) and higher level of violence Article 51 term “armed attack” being, as the Court in *Nicaragua* describes, the “most grave forms of the use of force.”<sup>86</sup> While not ignoring state practice, the Scale and Effects School’s analysis focuses more on the text and judicial decisions.<sup>87</sup>

Michael N. Schmitt, the Director of the project, wrote, “[t]he IGE worked assiduously to be objective”; further, “any claims that Tallinn Manual 2.0 takes this or that position should be viewed with a degree of skepticism”; however, “States should conclude that either asserting the same position [as the Manual] is likely to be an easy sell, or challenging it is going to be an uphill battle.”<sup>88</sup>

The Manual consists of two types of text. “Black letter rules” [text in bold] required unanimity and are meant to reflect *lex lata* (the law as it exists), not *lex ferenda* (what the law should be) . . . The heart of the Manual is instead in its commentary. It is here that a rule, its terminology, and the legal rationale for finding that it represents *lex lata* is set forth. Just as important in the commentary is the discussion of the various opinions among the IGE as to the application of the rule and its interpretation. Although all members concurred in the text of a Rule, they sometimes differed over its meaning in particular circumstances.<sup>89</sup>

Understanding this approach, Rule 71 is most helpful in clarifying the IGE’s position on how to define “armed attack”: “A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects.”<sup>90</sup> Contained within this rule, the IGE comes to a number of

---

86. *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶¶ 191, 195 (June 27); Dinstein, *supra* note 32, at 100; Dapo Akande & Antonios Tzanakopoulos, *The International Court of Justice and the Concept of Aggression*, in *THE CRIME OF AGGRESSION: A COMMENTARY* 214, 217 (Claus Kreß & Stefan Barriga eds., 2016).

87. See TALLINN MANUAL 2.0, *supra* note 4, at 341.

88. Schmitt, *supra* note 22.

89. *Id.*

90. TALLINN MANUAL 2.0, *supra* note 4, at 339. Bold in original. See *supra*, note 68. Bold rules from the Manual indicate “‘black letter rules’ [that] required



important conclusions for the Scale and Effects School. First, an effects-based rather than means-based test to define armed attack: “the critical factor [is] the effects of a cyber operation, as distinct from the means used to achieve the effects.”<sup>91</sup> Second, concurring in the differentiation of the terms ‘armed attack’ and ‘use of force,’ “an ‘armed attack’ is not to be equated with the term ‘use of force’ . . . [a]n armed attack presupposes at least a use of force in the sense of Article 2(4).”<sup>92</sup> However, as noted by the [ICJ], not every use of force rises to the level of an armed attack.”<sup>93</sup> Third, the adoption of the “‘scale and effects’ [threshold test for armed attacks] drawn from the *Nicaragua* judgment.”<sup>94</sup>

By accepting the “scale and effects” test, the IGE is explicitly not adopting a physical damage requirement for an incident to be an armed attack.<sup>95</sup> However, it is clear that some of the IGE would go this far, as “[s]ome of the experts took the position that harm to persons or physical damage to property is a condition precedent to the characterization of an incident as an armed attack.”<sup>96</sup> Even without adopting a physical damage requirement, the Manual states, “the law is unclear as to the precise point at which the effects of a cyber operation qualify as an armed attack.”<sup>97</sup>

Whether my disagreement is with the Manual or perhaps simply some of the IGE, there are three incidents or hypotheticals where the IGE struggled to definitively see an action as an armed attack which should be viewed as such. First, in “the 2010 Stuxnet operation[,] in light of the damage the operation caused to Iranian centrifuges, some members of the [IGE] were of the view that it reached the armed attack

---

unanimity.” Commentaries are not in bold. *Hereafter*, the same bold/not bold distinction will be maintained for quotations from the Tallinn Manual.

91. *Id.* at 340; *see also* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶¶ 90–91 (1996); Hargrove, *supra* note 49, at 138.

92. TALLINN MANUAL 2.0, *supra* note 4, at 341.

93. *Id.*; Dinstein, *supra* note 32, at 100; Akande & Tzanakopoulos, *supra* note 86, at 219.

94. TALLINN MANUAL 2.0, *supra* note 4, at 341.

95. *Id.* at 342.

96. *Id.*

97. *Id.* at 341

threshold . . . [o]ther Experts took the contrary view.”<sup>98</sup> Second, for “a cyber incident directed against a major international stock exchange that causes the market to crash,” “some Experts were unprepared to label it as an armed attack because they were not satisfied that mere financial loss constitutes damage” sufficient for an armed attack.<sup>99</sup> Finally, while separately discussing the lack of application of the law of armed conflict (LOAC) to the 2007 cyber-attacks against Estonia, the IGE concurred, apparently without objection, that “the situation did not rise to the level of an armed conflict.”<sup>100</sup> Contrary to these views, all three scenarios, even under the internal logic of “scale and effects” test, should be considered armed attacks.

The Kingdom of the Netherlands has adopted a similar approach.<sup>101</sup> A July 5, 2019, letter from the Government of the Kingdom of the Netherlands to their Parliament laid out the Netherlands’ legal position on cyber operations: “[T]o determine whether an operation constitutes an armed attack, the scale and effects of the operation must be considered.”<sup>102</sup> Further, “[a]n armed attack is not the same as the use of force within the meaning of article 2(4) of the UN Charter.”<sup>103</sup> The Government of the Netherlands, while not seeing physical damage as required, seems to at least keep the threshold for armed attacks to “very serious non-material consequences”<sup>104</sup>:

A cyber-attack that has comparable consequences to an armed attack (fatalities, damage and destruction) can justify a response with cyber weapons or conventional weapons . . . There is therefore no reason not to qualify a cyberattack against a computer or information system as an armed attack if the consequences are comparable to those of an attack with conventional or non-conventional weapons. At present there is no

---

98. *Id.* at 342.

99. *Id.* at 343.

100. *Id.* at 376.

101. *See, e.g.*, Letter from the Government of the Kingdom of the Netherlands to the Parliament, 1, 4 (July 5, 2019) (available online) (English translation) <https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf> [Hereinafter Netherlands Letter] (discussing the Netherlands’ obligations under international law regarding cyberspace).

102. *Id.* at 8.

103. *Id.*

104. *Id.* at 9.

international consensus on qualifying a cyberattack as an armed attack if it does not cause fatalities, physical damage or destruction yet nevertheless has very serious non-material consequences.<sup>105</sup>

While not wholly ruling out the possibility of a cyber operation that lacked physical effects being an armed attack, by specifically citing “fatalities, damage and destruction,” the government of the Netherlands seemed more reticent than the IGE.<sup>106</sup> While the Netherlands’ letter does not analyze specific hypotheticals, the government’s position appears to be falling on the more restrictive end of the spectrum of the IGE, perhaps still reading a cyber-attack caused stock market crash as “very serious non-material consequences.”<sup>107</sup> In the Netherlands’ analysis defining of “use of force,” the farthest the government would go is, “at this time *it cannot be ruled out* that a cyber operation with very serious financial or economic impact *may* qualify as a use of force.”<sup>108</sup> If the Netherlands is hesitant to conclusively define “very serious financial or economic impact” as even a use of force, it seems unlikely the government would define it as an armed attack, despite later holding out the possibility.<sup>109</sup>

This notion, that even within the scale and effects test a cyber operation must have some physical effects, has some important adherents in a 2012 article co-written by Michael Schmitt and others: “[a]lthough there is no bright-line scale-and-effects test to distinguish grave from nongrave consequences, legal experts generally agree that to qualify as an armed attack, a cyber-attack must result in death or a significant degree of injury to persons or physical damage to property.”<sup>110</sup>

The debate within the Scale and Effect School is not simply a division between a physical effect or not, as evidenced by the IGE’s lack of consensus over how to define the Stuxnet operation, which obviously did have physical effects.<sup>111</sup> Even when physical effects are

---

105. *Id.* at 8.

106. *Id.*

107. *Id.* at 9.

108. *Id.* at 4.

109. *Id.*

110. William H. Boothby et al., *When is a Cyberattack a Use of Force or an Armed Attack?*, 45 COMPUT. SOC’Y 82, 83 (2012).

111. See TALLINN MANUAL, *supra* note 4, at 342. See generally Kim Zetter, *An*

present, some would still find them below the level of an armed attack, in what the Court in *Nicaragua* regrettably labels “mere frontier incidents.”<sup>112</sup> Those adopting the Court’s frontier incidents logic could divide over scale regardless of the presence of physical effects—perhaps viewing Stuxnet as not an armed attack, despite physical damage, and a total stock market crash as an armed attack, in spite of no physical damage.<sup>113</sup>

There is somewhat of an artificial yet important barrier between the Scale and Effects and the Forceful Countermeasure Schools, which is the lawfulness of forceful countermeasures in the space between a use of force and an armed attack.<sup>114</sup> “A contentious issue with respect to the limitations on countermeasures is whether they may consist of actions that amount to a use of force.”<sup>115</sup> This distinction is somewhat artificial, because

all the members of the [IGE] agreed that countermeasures may not rise to the level of an armed attack . . . they were divided over whether cyber countermeasures crossing the use of force threshold but not reaching that of an armed attack, are lawful . . . the majority of the [IGE], the obligation to refrain from the use of force is a key limitation on an injured State when conducting countermeasures.<sup>116</sup>

Despite the debate within the IGE, I will attribute the majority opinion of the IGE to the Scale and Effect School and the minority opinion to the later discussed Forceful Countermeasures School. This distinction is important because the remedies open to a victim state under each school would be vastly different.

## VI. PROBLEMS WITH SCALE AND EFFECTS

---

*Unprecedented Look at Stuxnet, the World’s First Digital Weapon*, WIRED (Nov. 3, 2014), <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/> (noting that Stuxnet “escaped the digital realm to wreak physical destruction on equipment the computers controlled”).

112. *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 195 (June 27).

113. TALLINN MANUAL, *supra* note 4, at 342 (specifying that all Experts found Stuxnet to be a use of force, while some also considered it to be an armed attack).

114. See Efrony & Shany, *supra* note 82, at 591.

115. TALLINN MANUAL, *supra* note 4, at 125.

116. *Id.*

## SCHOOL

The Scale and Effects School, as advanced in the Tallinn Manual, explicitly described by Michael Schmitt, is only attempting to be descriptive, not prescriptive.<sup>117</sup> The Scale and Effects School makes a concerted effort to read the Charter honestly, informed by relevant opinions of the ICJ.<sup>118</sup> But by leaving a gap between Articles 2(4) and 51, and a wide gap at that, the Scale and Effects School leaves only three unworkable outcomes: 1) a system where a state that is a victim of a cyber-attack not rising to an armed attack can do little more than complain to the Security Council, 2) the likely unsuccessful, use of countermeasures short of force, or 3) the unlawful use of counterforce.<sup>119</sup> None produce a satisfying or realistic result. Divining the future is always challenging, but this author views setting such a high bar for a forceful response as more likely to encourage violence, than discourage it.<sup>120</sup>

A functionalist look at the Charter exposes the illogical conclusion of the supposed objective, the senseless, strict textualism of the Scale and Effects School.<sup>121</sup> That supposed textualist reading cannot be correct because of the size of this unrealistic gap, particularly in our three scenarios, is akin to 1) Stuxnet, 2) a stock-market crash, and 3) the 2007 Estonia attacks. The Scale and Effects School fails predictively, descriptively, and prescriptively. Predictively, states *will not* adhere to the overly rigid standard form of scale and effects—making most states lawbreakers.<sup>122</sup> Descriptively, the *Nicaragua*

---

117. See Silver, *supra* note 3, at 80.

118. See TALLINN MANUAL, *supra* note 4, at 340.

119. Under the Scale and Effects School, states could also use non-forceful countermeasures, as well as attempts to mobilize international political support, or international condemnation for the aggressor state. Interestingly, this would likely resemble the actions a weaker state would employ against more powerful states, even if the actions were viewed as an armed attack, regardless of how the law is viewed. Estonia's response in 2007 may be an example. See *id.* at 333, 337.

120. See Efrony & Shany, *supra* note 82, at 590 (discussing the counterintuitive outcome of a narrow definition of "use of force").

121. Cf. TALLINN MANUAL, *supra* note 4, at 341 (noting that "the parameters of the scale and effects criteria remain unsettled beyond the indication that they need to be grave").

122. See Franck, *supra* note 10, at 837 (predicting that the rules "will bend and break" so long as nations have interests that run counter to stated international legal norms).

decision is inherently flawed, particularly when applied to cyber operations.<sup>123</sup> Moreover, despite a claimed effects-based analysis, there is a means-based bias baked into the Scale and Effects School—bombs are inherently more likely to break things than code. Even accepting the test as enumerated, the Tallinn Manual's analysis is flawed.<sup>124</sup> Stronger answers can be found by comparing cyber-attacks to conventional means that would have similar effects: a) Is a denial of service more like frequency jamming or destroying communication lines? b) Is an attack that closes a state off from commerce more like economic sanctions or a blockade? c) Is invasive malware more like espionage or sabotage? Finally, prescriptively, even if you retain some of the separation between armed attack and other lower uses of force, as the language of the Charter *might* support, the principle of proportionality is a better, more workable guide than the logic of *Nicaragua*.<sup>125</sup>

#### A. PREDICTIVE PROBLEMS.

Why is predictability important? It is highly likely that many legal thinkers (particularly of international law) would find it far simpler to look into the past, at treaties, practice (customary law), and legal decisions and discern what the law *is*, but this leaves out critically forward-looking analysis. Past state practice obviously has a primary role in the making of law, but what is the purpose of a description of law that will be certainly ignored? This begs a philosophical question: Can a rule that no one believes will be followed truly be law? “It is not enough that the [the primary rules] be internally coherent: they must be intrinsically compelling.”<sup>126</sup> This a key failure of the Scale and Effect School, particularly as applied to cyber operations.

Thankfully, a wide scale, long-term nation-crippling cyber-attack has not occurred,<sup>127</sup> but suppose a large scale and persistent cyber-attack upon the stock exchange or financial institutions of a country does happen, causing widespread and ongoing financial collapse –

---

123. Silver, *supra* note 3, at 81.

124. See Peter Z. Stockburger, *Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum*, 31 AM. U. INT'L L. REV. 546, 579–80 (2016).

125. See TALLINN MANUAL 2.0, *supra* note 4, at 352.

126. Hargrove, *supra* note 49, at 137.

127. Silver, *supra* note 3, at 78.

stock values crater, all investment effectively stops, electronic means of payment cease functioning, workers cannot be paid, citizens are unable to access funds in bank accounts – but no physical damage occurs, and the attack is clearly and unambiguously attributable to another state.<sup>128</sup> No one would realistically argue that a victim state would not stop the attack if they had the means, either kinetic or cyber.<sup>129</sup> While, again, some of the Scale and Effects School would see such a nation-crippling act as rising to an armed attack, clearly some of the IGE wouldn't go this far.<sup>130</sup> Assuming all would agree that any state would respond in *claimed* “self-defense” when vitally threatened with force, what would be the purpose of a law that would a) come to such an illogical conclusion and b) be so likely disregarded? Few states would admit to law-breaking; rather, their justification would simply be that the attack rose to the level of an armed attack, justifying self-defense. Such a rule, that will predictively be disregarded, while given lip-service, is just as unhelpful.<sup>131</sup>

More likely than the hypothetical large-scale attack would be so-called “pin-prick” attacks, a series of smaller, far less damaging but repeated attacks, again without physical damage.<sup>132</sup> The Tallinn Manual struggles on how to view these attacks, asking should they be viewed collectively or individually?<sup>133</sup> But the problem remains the same, “a paper rule”<sup>134</sup> that will be disregarded cannot be the rule:

---

128. *Id.* at 73, 77–78. Realistically, attribution will always be the most difficult matter, both factually and in terms of state responsibility. These issues, although highly interesting, are beyond the scope of this writing.

129. Schmitt, *supra* note 22 (noting that the rules coming out of the Tallinn Manual capture the reasonable position nations can take).

130. See TALLINN MANUAL 2.0, *supra* note 4, at 343 (showing the differing position of the Experts regarding labeling an attack an armed attack).

131. Silver, *supra* note 3, at 83 (“Such a position would either legalize under Article 2(4) a broad range of hostile and destructive acts that fail to reach the armed attack threshold or would provide an incentive to lower the Article 51 threshold old, with a concurrent risk of expanding violence under the pretext of legitimate self-defense.”).

132. See CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 107 (2000) (explaining use of the “pin-prick” theory by states justifying responses to armed attacks).

133. See generally TALLINN MANUAL 2.0, *supra* note 4, at 342 (agreeing that a determinative factor turns on if the attacks are linked and have the same origin).

134. Michael J. Glennon, Debate with Alain Pellet: Force and the Settlement of Political Disputes, *The Hague Academy of International Law* 7 (Sept. 7, 2007),

“paper rules may still in some circumstances generate compliance—but not often enough to qualify as law, for the key element of obligation is missing.”<sup>135</sup>

Admittedly, this is applying a forward-looking version of the Charter-Is-Dead School’s view of past state practice, but the value is the same. There must be some linkage between law and practice, past or predictively future.<sup>136</sup> If the scale and effects test is to survive, all consideration of physical effects must be jettisoned; when speaking of “gravity,”<sup>137</sup> the entire “consequences,” as used in The Netherlands letter, of a cyber operation must be considered.<sup>138</sup> All states will not use force in self-defense, but it is unlikely that *law* (under scale and effects) is what will restrain them.<sup>139</sup> As with the 2007 Estonia attacks, political considerations and real-world power dynamics will be the deciding factors.<sup>140</sup> Because of the waffling found in the Tallinn Manual and the Netherlands legal opinion, the Scale and Effects School provides little predictive value.<sup>141</sup> In fact, the predictive reality is that, contrary to the rule, states will use self-defense when vital interests are threatened and will justify their action as a response to an armed attack despite (not because of) the scale and effects test.<sup>142</sup>

## B. DESCRIPTIVE PROBLEMS.

My objections to the descriptive value of Scale and Effects School, at its core, are twofold: 1) The scale and effects test as conceived by

---

[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1092212](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1092212) (citing, Roscoe Pound, *Law in Books and Law in Action*, 44 AM. L. REV. 12 (1910)).

135. *Id.* at 7.

136. See Silver, *supra* note 3, at 82 (discussing the applicability of past laws in reference to newer technologies and challenges).

137. See generally Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 228 (June 27); Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶ 72 (Nov. 6) (separate opinion by Simma, J.).

138. Netherlands Letter, *supra* note 101, at 4, 8.

139. See TALLINN MANUAL 2.0, *supra* note 4, at 331, 339 (explaining the factors of the “scale and effects” test when determining whether a state should respond in self-defense).

140. Accord McGuinness, *supra* note 30 (explaining the 2007 Estonian attack).

141. See generally TALLINN MANUAL 2.0, *supra* note 4, at 330–31, 333–34 (noting the wide range of outcomes that can result from using the use of force factors).

142. *Id.* at 339.



the Court in *Nicaragua* should not be the test, and 2) even assuming the logic of the Court is correct, as applied by the Tallinn Manual to cyber operations, it fails to value cyber property correctly.

*i. Problems with Scale and Effects, as conceived.*

While the desire is not to conduct a full-fledged analysis of the weaknesses of *Nicaragua* and its logic, continued into its progeny *Oil Platforms*, it is necessary to stop and ponder this misstep of judgeship—"a misfortune of some magnitude" that was "deeply unwise"—and why it should be disregarded whole cloth.<sup>143</sup> First, obviously and fundamentally, as with all ICJ opinions, its decisions have no precedential value and are only binding on the parties concerned and only for the current matter.<sup>144</sup> From a starting point, the decision should simply be viewed as a foul ball—an event that occurred, but should have no bearing on the rest of the game.

The *Nicaragua* Court attempts to deal with the admitted language difference between "use of force" from Article 2(4) and "armed attack" from Article 51, but the case is a poor vehicle for that distinction.<sup>145</sup> The court in *Nicaragua* was jurisdictionally limited to customary law claims because of U.S. reservations when assenting to the Statute of the ICJ.<sup>146</sup> While the court asserts, in concordance with the U.S. position, that customary international law is congruent with the Charter, but because the court is only able to pass judgment on what customary law is, the court cannot answer, beyond dicta, what that the law under the Charter actually is—further limiting whatever precedential value one might give it.<sup>147</sup> While state practice (coupled with *opino juris*) can certainly modify treaty law, actual practice must

---

143. See Hargrove, *supra* note 49, at 140 (questioning the holding of *Nicaragua* and its impact on international law).

144. See Statute of the International Court of Justice, art. 59 [hereinafter ICJ Statute] ("The decision of the Court has no binding force except between the parties and in respect of that particular case.").

145. See *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶¶ 33, 51, 56, 173, 190 (June 27).

146. *Id.* ¶ 182.

147. *Id.* ¶ 187; see also Hargrove, *supra* note 49, at 137 ("The Court put itself into a position that required it to apply exclusively customary international law, largely derivative from the United Nations Charter but nevertheless separate.").

be given a larger focus when determining customary law.<sup>148</sup> Beyond stating that the U.S. views the language of the Charter to be customary law, the Court does not meaningfully engage in an effort to consider state practice.<sup>149</sup> Beyond whatever the Court and U.S. mean that the language of the Charter is customary law, are not the particulars of how the U.S. (and all other states) *interpret* (i.e. *opinio juris*) the Charter, the real question that would need to be considered to find customary law?

Here, the Court makes the assertion:

[I]f a State acts in a way *prima facie* incompatible with a recognized rule, but defends its conduct by appealing to exceptions or justifications contained within the rule itself, then whether or not the State's conduct is in fact justifiable on that basis, the significance of that attitude is to confirm rather than to weaken the rule.<sup>150</sup>

While, certainly, a state claiming “the State’s conduct is in fact justifiable”<sup>151</sup> strengthens the argument that there is *a* rule, it does the opposite of what the court claims: it strengthens the claim that the rule, or at least the state’s interpretation of that rule, is what the state claims it to be.<sup>152</sup> If sufficient state practice and *opinio juris* exist for the new or even original, correct interpretation, although potentially textually inconsistent with the Court’s interpretation of the rule, then the rule is what the *prima facie* “rule-breaker” says it is.<sup>153</sup> One needs not go wholly over to the Charter-is-Dead School to see the obvious problem of the ubiquitous state practice of justifying “self-defense” in situations the *Nicaragua* Court would label as “mere frontier incident[s].”<sup>154</sup>

The reason the Court needed to distinguish “most grave forms of the use of force” versus “other less grave forms”<sup>155</sup> was to determine whether the United States’ actions could have been justifiable as

---

148. *Nicaragua*, 1986 I.C.J. 14, ¶ 184.

149. *Id.* ¶¶ 173–74.

150. *Id.* ¶ 186.

151. *Id.*

152. *Id.*

153. *Id.*

154. *Id.* ¶ 195.

155. *Id.* ¶ 186.

collective self-defense.<sup>156</sup> The court adds a requirement to collective self-defense that the “state which is the victim of an armed attack which must form and declare the view that it has been so attacked.”<sup>157</sup> The court would clearly apply the same “scale and effects” threshold test as the predicate for either individual or collective self-defense;<sup>158</sup> however, it is also clear that the court took into consideration that Costa Rica and Honduras never directly alleged to be the victim of an armed attack,<sup>159</sup> and El Salvador only claimed to be the victim of an armed attack long after the alleged incidents occurred.<sup>160</sup> The question of self-perceived victimhood would not be helpful to individual self-defense, as this entire discussion concerning what level of force justifies self-defense would be moot if the targeted state (and one-in-the-same, responding state) did not even believe it was the victim of an armed attack.<sup>161</sup> Even if still using “scale and effects,” it is interesting to consider if the court’s judgment would have viewed the actions of Nicaragua as not rising to an armed attack, if one or all of the three states concerned (Costa Rica, Honduras, or El Salvador) would have immediately: 1) declared their perceived victimhood of an armed attack and 2) responded with individual self-defense.<sup>162</sup>

Despite the court attempting to separate the analysis of defining an armed attack (i.e., scale and effects)<sup>163</sup> as distinct from attribution to a state (i.e., effective control),<sup>164</sup> it is clear the court bled the concepts together:

Even assuming that the supply of arms to the opposition in El Salvador could be treated as imputable to the Government of Nicaragua, to justify invocation of the right of collective self-defence in customary international law, it would have to be equated with an armed attack by Nicaragua on El Salvador . . . Even at a time when the arms flow was at its peak, and again assuming the participation of the Nicaraguan Government, that would not

---

156. *Id.* ¶ 193.

157. *Id.* ¶ 195.

158. *Id.*

159. *Id.* ¶ 234.

160. *Id.* ¶ 233.

161. *Id.* ¶ 195.

162. *Id.* ¶¶ 233–34.

163. *Id.* ¶ 195.

164. *Id.* ¶ 116.

constitute such armed attack.<sup>165</sup>

Further evidence that the Court conflates gravity with responsibility, the United States' "mere supply of funds to the *contras* while undoubtedly an act of intervention in the internal affairs of Nicaragua, . . . does not in itself amount to a use of force."<sup>166</sup> The Court conflates the supply of funds with the *actus reus* of a use of force, which it certainly is not, with state responsibility, which it very well could be. Judge Yusuf argued in 2012 that the Court was never even defining "armed attack,"<sup>167</sup> if true, then 1) *Nicaragua* should be disregarded as to definition of "armed attack," and 2) the Court's language seriously confused the issue.<sup>168</sup>

However, the Court is not alone in this blending. In UN General Assembly Resolution 3314, the Assembly in their definition of aggression included in Article 3, "The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State; and (g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above."<sup>169</sup>

---

165. *Id.* ¶ 230.

166. *Id.* ¶ 228.

167. See Abdulqawi A. Yusuf, *The Notion of 'Armed Attack' in the Nicaragua Judgement and Its Influence on Subsequent Case Law*, 25 LEIDEN J. INT'L L. 461, 461, 465 (2012) ("It is my view that the clearest understanding of the Court's definition of an 'armed attack' in *Nicaragua* is to be had by situating it in its context: the Court was presented with a specific task, namely to adjudicate a dispute concerning 'armed bands' acting under the auspices of another state, and to determine the conditions necessary for a justifiable exercise of collective self-defence. Thus, the issue presented was not to define an armed attack proper (i.e., at the hands of regular armed forces of a state), or even an armed attack by unaffiliated irregulars, but rather to characterize acts of force carried out by indirect means and through irregular forces that may justify the exercise of collective self-defence."); see also Yusuf, *supra*, at 466 ("The *Nicaragua* definition of an 'armed attack' by the Court could have been construed as applicable only to indirect uses of force and to collective self-defence if the Court itself did not expand the scope of application of the standard it formulated in *Nicaragua* in its subsequent judgment in *Oil Platforms*.").

168. *Nicaragua*, 1986 I.C.J. 14, ¶¶ 116, 195, 228, 230.

169. G.A. Res. 3114 (XXIX), art. 3 ¶¶ (f)–(g) (Dec. 14, 1974); see also Akande

The Court in the *Oil Platforms* case, following the example from *Nicaragua* continued to mix the idea of responsibility with gravity when it could not even definitively conclude that the mining of a naval vessel would constitute an armed attack.<sup>170</sup>

The Court does not exclude the possibility that the mining of a single military vessel might be sufficient to bring into play the 'inherent right of self-defence'; but in view of all the circumstances, including the inconclusiveness of the evidence of Iran's responsibility for the mining of the *USS Samuel B Roberts*, the Court is unable to hold that the attacks on the *Salman* and *Nasr* platforms have been shown to have been justifiably made in response to an 'armed attack.'<sup>171</sup>

The "inconclusiveness of the evidence" may very well lead one to see a lack of definitive responsibility on behalf of Iran, thus not justifying a U.S. response, but responsibility should have nothing to do with definitively stating that mining a naval vessel *is* an armed attack, at least if honestly judged by its scale and effects.<sup>172</sup>

Because the question of attribution is all the more present in cyber-operations, there must be even more diligence in separating the analysis of attribution and threshold.<sup>173</sup> Reading *Nicaragua* more generously than is accurate, Taft asserts in an analysis of *Oil Platforms* "[t]here is nothing in the Court's discussion . . . implying that missile and mine attacks on naval and commercial vessels are anything less than an armed attack."<sup>174</sup> Unfortunately, with the creation of "mere frontier incidents," that is exactly what the *Nicaragua* Court claims the law to be.<sup>175</sup>

---

& Tzanakopoulos, *supra* note 86, at 8–9 ("[T]he Court has referred, almost constantly, to the concept of aggression, and particular to . . . GA Resolution 3314 . . . What becomes clear is that the Court considers the concepts of armed attack and aggression to be at least cognate.").

170. *Oil Platforms* (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶ 64 (Nov. 6) (separate opinion by Simma, J.).

171. *Id.* ¶ 72.

172. *Id.*

173. See Dinstein, *supra* note 32, at 111 (describing the importance of attribution for states to use counter-measures).

174. William H. Taft IV, *Self-Defense and the Oil Platforms Decision*, 29 YALE J. INT'L L. 295, 302 (2004) [hereinafter Taft, *Self-Defense*].

175. *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 195 (June 27).

Accepting the courts' general framing, the test must meet two separate prongs: first, the Court should determine if the violence threshold for an armed attack was crossed (using scale and effects); then, determine if the attack should be attributed to the state (using effective control).<sup>176</sup> So, the question should not be: Does the supply of arms to the El Salvadorian opposition constitute an armed attack? Rather, using scale and effects: Do the actions of the El Salvadorian opposition constitute an armed attack? *Then*, using effective control: Should the actions of the El Salvadorian opposition be attributed to Nicaragua? There is a potential debate over whether a non-state actor can even commit an armed attack,<sup>177</sup> perhaps requiring a reversal of the order of the two prongs. I am agnostic; however, under the Scale and Effects School framing, "armed attack" is a gravity question and should not be confused with responsibility. So regardless of the order of the application of the test, the analysis must be separate. In some situations, attribution will be obvious, such as when the military of State A attacks the military of State B. In more difficult scenarios, terrorists or hacktivists may be operating from State C with support from State A, against State B. Under either prong, the test may fail, but they must be kept apart, analyzed separately, and not comingled.<sup>178</sup>

Even if one accepts the general textual proposition of the Scale and Effects School—that there is a gap between Arts. 2(4) and 51, there should still be further doubts about the logic of the size of that gap created by the Court in *Nicaragua*. The Court does attempt to deal with the language discrepancy between "use of force" and "armed attack," but by using wholly created terms like "most grave" and "mere frontier incident,"<sup>179</sup> the Court seems to be seeking a

---

176. *Id.* ¶¶ 115, 195.

177. See TALLINN MANUAL 2.0, *supra* note 4, at 340 (noting that "[w]hether non-State actors may initiate an armed attack as matter of law is the subject of some controversy").

178. See Yusuf, *supra* note 167, at 462 ("[T]he definition of 'armed attack' is itself problematic, because the Court's evaluation . . . frequently occurs within the broader discussion of self-defence. Thus, the question necessarily tends toward whether self-defence was justified, and not just whether an armed attack occurred in the objective sense of the question."); see also *id.*, at 463 ("The Court has been criticized for weakening the prohibition of the use of force, while on the other hand, it has been accused of undermining the right of self-defence.").

179. *Nicaragua*, 1986 I.C.J. 14, ¶ 191.

predetermined bias toward limiting situations justifying self-defense. Interestingly, while not congruent with an armed attack, this bias against seeing force for what it is, is on display in that, “the Court has never qualified an unlawful use of force as an act of aggression.”<sup>180</sup>

Silver rejects this framing, attributing the bias, at least of some scholars favorable of the opinion, toward broadening the gap for non-conventional attacks to a fear of a “slippery slope” to “applying Article 2(4) to measures of economic and political coercion that have similarly devastating effects.”<sup>181</sup> While honestly dealing with the terms as different, the Court does not honestly deal with any plain language meaning of the words “armed” or “attack.”<sup>182</sup> Admittedly, dictionary lawyering is always one of the lowest forms, but according to Merriam-Webster, “armed” means: “furnished with weapons, *also* : using or involving a weapon”<sup>183</sup>; and “attack” means: “to set upon or work against forcefully.”<sup>184</sup> Any reasonable understanding of these words could easily describe an incident of a scale the Court would consider a frontier incident.<sup>185</sup> Any force of a military nature should be viewed, *definitionally*, as an armed attack.

The premise underlying the proposition that some acts of force cannot be resisted by force in self-defense is that, because the language of Article 51 is not identical to that of Article 2(4), some acts of unlawful force are not to be regarded as “armed attacks.” That premise is otherwise unsupported by the language of the Charter, and simply imposes its distinctions on the

---

180. Akande & Tzanakopoulos, *supra* note 86, at 5.

181. Silver, *supra* note 3, at 83 (arguing that it is better to find activities, when similar to military force in its destructive nature, fall into the scope of Article 2(4)).

182. *Nicaragua*, 1986 I.C.J. 14, ¶ 195.

183. See *Armed*, MERRIAM-WEBSTER, <https://www.merriam-webster.com/dictionary/armed?src=search-dict-box>, (last visited Mar. 8, 2020) (defining armed).

184. See *Attack*, MERRIAM-WEBSTER, <https://www.merriam-webster.com/dictionary/attack> (last visited Mar. 8, 2020) (defining attack).

185. See SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA art. 13 (Louise Doswald-Beck ed., 1995) [hereinafter SAN REMO MANUAL] (noting that the San Remo Manual appears careful to avoid the term “use of force” instead using simply the term “attack,” which it defines as “an act of violence, whether in offence or in defence,” seeming to be closer to how both the Court in *Nicaragua* and the Tallinn Manual would define “use of force,” lending further support to the notion that a better definition of “armed attack” is simply “an armed act of violence,” rather than including the addition of a gravity requirement).

plain language of Article 51, which in no way limits itself to especially large, direct or important armed attacks. The Court itself offered nothing that ameliorates the arbitrariness of its pronouncement. At one point it erroneously invoked, in a surprising misreading, the General Assembly's Definition of Aggression.<sup>186</sup>

While no scholar advances, nor do I here, but, from a purely textualist approach, a possible interpretation of the words "armed attack" is as lower level force term, not higher; or, perhaps, use of the word "armed" is simply intended to separate armed versus unarmed force? Whatever one makes of these words, the Court simply created a gravity requirement in Article 51 that is not present in state practice, considering that all the Court had jurisdiction to hear was customary law.<sup>187</sup> If there is a gap, as the Court asserts, it is certainly narrower than claimed.<sup>188</sup>

## *ii. Problems with Scale and Effects, as applied*

The unreasonably high threshold of the scale and effects test becomes obvious in the *Oil Platform* case's holding, "[e]ven taken cumulatively, and reserving, as already noted, the question of Iranian responsibility, these incidents do not seem to the Court to constitute an armed attack on the United States, of the kind that the Court, [in *Nicaragua*] qualified as a 'most grave' form of the use of force."<sup>189</sup> The Court looked at the following:

[T]he mining of the United States-flagged *Bridgeton* on 24 July 1987; the mining of the United States-owned *Texaco Caribbean* on 10 August 1987; and firing on United States Navy helicopters by Iranian gunboats, and from the Reshadat oil platform, on 8 October 1987[, . . . finding] the *Iran Ajr*, in the act of laying mines in international waters some 50 nautical miles north-east of Bahrain.<sup>190</sup>

---

186. Hargrove, *supra* note 49, at 139.

187. *Id.* at 299–300.

188. See Dinstein, *supra* note 32, at 100 (agreeing that that there is an intentional gap between Arts. 2(4) and 51, but that "the gap has to be quite narrow, inasmuch as 'there is very little effective protection against states violating the prohibition of the use of force, as long as they do not resort to an armed attack'").

189. *Oil Platforms (Iran v. U.S.)*, Judgment, 2003 I.C.J. 161, ¶ 64 (Nov. 6) (separate opinion by Simma, J.).

190. *Id.* ¶ 66.



These events cumulatively did not rise to an armed attack. Another U.S. flagged tanker struck with a Silkworm missile was also not considered an armed attack.<sup>191</sup> This simply cannot be; “there is no support in international law or practice for the suggestion that missile and mine attacks carried out by a State’s regular armed forces on civilian or military targets of another State do not trigger a right of self-defense.”<sup>192</sup> One could accept that the language of the Charter creates the claimed gap, but the threshold for an “armed attack” definitionally cannot exclude clear acts of war, the likes of those both Courts excluded.<sup>193</sup>

When conventional force is used by regular militaries, responsibility is unlikely to be unclear, but in the cyber domain, much like irregular or guerrilla warfare in *Nicaragua* state responsibility will likely be the most challenging factual and legal analysis.<sup>194</sup> That is why, if following the scale and effects test, the gravity analysis must be fully separated from the responsibility analysis. While seemingly obvious, it also seems that neither the Courts in *Nicaragua* nor *Oil Platforms* did so, instead looking at the acts that would lead to responsibility and judging if those acts constituted sufficient gravity.<sup>195</sup> Again, “the mere supply [of arms] . . . does not in itself amount to a use of force.”<sup>196</sup> While this assertion is correct, framing the question as such mixes gravity with responsibility.<sup>197</sup> Because of the possibility of hidden responsibility through the use of “hacktivist groups” or even cyber soldiers of fortune and the ability to co-opt computers from one or more third states, the state responsibility analysis will be incredibly situational and fact specific, thereby beyond the scope of this writing.<sup>198</sup> However, it is unthinkable to imagine any state believing there was *opinio juris* or acting in a manner where they could not respond with sufficient force to stop

---

191. *Id.* ¶ 64.

192. Taft, *Self-Defense*, *supra* note 174, at 302.

193. See Dinstein, *supra* note 32, at 100 (explaining that the gap is created because illegal uses of force are not always equal to armed attacks between states).

194. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 115 (June 27).

195. *Id.* ¶ 228.

196. *Id.*

197. *Id.*

198. *Id.* ¶ 115.

enemy soldiers on one side of a border checkpoint shooting at soldiers on the other side—what the Court in *Nicaragua* might label only a frontier incident.<sup>199</sup>

Despite claiming in the Tallinn Manual and in *Nicaragua* that scale and effects should be an effects-based, not means-based analysis, applied by the IGE and the Netherlands, there is an inherent bias against non-kinetic means because the *effects* the Scale and Effects School looks for are death and destruction.<sup>200</sup> Inherently, the means of cyber operations, the use and manipulation of data, and, equally, the presumed desired effects, such as Stuxnet, stock market crashes, and the 2017 Estonia attacks, do not produce the type of effects (death and bomb-like physical destruction) of the Scale and Effects School.<sup>201</sup> A better application would be to look at the scale and effects, not in physical terms, as the Manual disclaims yet still seeks, but in overall terms.<sup>202</sup> There may be large-scale invasions that, while causing numerous casualties, are easily repulsed, but do not produce the scale and effects in terms of national risk and damage created by an economic-targeted cyber-attack. While the Court in *Oil Platforms* fails to conclusively hold that the mining of a single warship would constitute an armed attack, it is likely that Iran saw the scale and effects of the Stuxnet operation as far more strategically damaging.<sup>203</sup> The Government of the Netherlands letter's use of the word "consequences" is possibly the better framing of the Court's scale and effects test.<sup>204</sup>

---

199. *Id.* ¶ 195.

200. *Id.*; TALLINN MANUAL 2.0, *supra* note 4, at 340–41; *see* Dinstein, *supra* note 32, at 103 ("A [cyber-attack] can qualify as an armed attack just as much as a kinetic attack bringing about the same—or similar—results. The crux of the matter is not the medium at hand . . . but the violent consequences of the action taken."); *see also* Silver, *supra* note 3, at 88 (discussing Michael Schmitt's differentiation between "instrument-based" and what will ultimately become the effects-based test found in the Tallinn Manual).

201. TALLINN MANUAL 2.0, *supra* note 4, at 342–43.

202. *See* Silver, *supra* note 3, at 88.

203. *Oil Platforms* (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶ 72 (Nov. 6) (separate opinion by Simma, J.).

204. *See* Netherlands Letter, *supra* note 101. *But 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, 911 (1999). ("In fact, the international community is not directly concerned with the particular coercive

## VII. HOW TO BETTER THINK ABOUT SCALE AND EFFECTS OF CYBER OPERATIONS.

Here, one cannot ignore a fundamental disagreement within the Scale and Effects School regarding the view of physical effects for an armed attack.<sup>205</sup> Without constructing an artificial strawman, clearly only some of the IGE “took the position that harm to physical damage or property is a condition precedent to the characterization of an incident as an armed attack.”<sup>206</sup> For this group, the assertion that their test is “effects”-based, is in name only.<sup>207</sup> Writing elsewhere, regarding the targeting of civilian objects, the Manual discusses what the IGE considers to be an object: “The majority of the [IGE] agreed that the law of armed conflict notion of ‘object’ is not to be interpreted as including data.”<sup>208</sup> In agreement with the International Committee of the Red Cross’s (ICRC’s) definition of “object” as “visible and tangible in the 1987 Commentary to Additional Protocols of 1977,”<sup>209</sup> the Manual continues:

Therefore, an attack on data *per se* does not qualify as an attack. They [the majority of the IGE] agreed, however, that, . . . a cyber operation targeting data may sometimes qualify as an attack when the operation affects the functionality of cyber infrastructure or results in other consequences that would qualify the cyber operation as an attack.<sup>210</sup>

Admittedly, the minority of the IGE disagreed.<sup>211</sup> While it is not noted how individual members of the IGE “voted,” it stems to reason that there was a high degree of overlap between those who saw data

---

instrumentality used (force in this case), but rather the consequences of its use. However, it would prove extraordinarily difficult to qualify consequences in a normative practical manner. Undesirable consequences fall along a continuum, but how could the criteria for placement along it be clearly expressed?”).

205. TALLINN MANUAL 2.0, *supra* note 4, at 342.

206. *Id.*

207. *Id.*

208. *Id.* at 437.

209. CLAUDE PILLOUD ET AL., INT’L COMM. OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 633 (1987) [hereinafter, ICRC Commentaries to Additional Protocols]; *see also* Dinstein, *supra* note 32, at 102 (“The likelihood of a [cyber-attack] ever constituting a full-fledged armed attack would be scant.”).

210. TALLINN MANUAL 2.0, *supra* note 4, at 437.

211. *Id.*

as not an object also saw a requirement of physical damage for an armed attack.<sup>212</sup> There are two better ways, while using the built-in logic of the Tallinn Manual, to apply the scale and effects test.<sup>213</sup> First, the simplest, and most realistic, application is that data is a physical object.<sup>214</sup> Second, even if data is not considered an object, the test should clearly include, and value appropriately, non-physical effects of cyber operations.<sup>215</sup> Regardless of which path one takes, one should end up at a more appropriate and defensible position.<sup>216</sup>

First, taking the position that data is an object certainly simplifies some of the tortured logic of the scale and effects analysis as applied by the Tallinn Manual.<sup>217</sup> The most obviously problematic scenario is a cyber-attack on a stock exchange that causes wide-spread financial damage, perhaps even crippling the nation, without causing any physical damage—the very scenario both the Tallinn Manual and the Government of the Netherlands appeared conflicted over.<sup>218</sup> If digital data is an object, clearly destroying the data that made up a stock market would reach the scale and effects of an armed attack.<sup>219</sup> Whether data is an object is mostly a conceptual question.<sup>220</sup> There are two main reasons why data should be viewed as an object: first, literally, and second, practically.<sup>221</sup>

From the most purely literal and technical perspective, although we talk about data as though it as an amorphous non-spatial form that is everywhere and nowhere, this assumption is not true.<sup>222</sup> Despite its

---

212. *Id.*

213. *Id.*

214. *Id.*

215. *Id.* at 334.

216. See, e.g., Michael J. Adams, *A Warning About Tallinn 2.0 . . . Whatever it Says*, LAWFARE (Jan. 4, 2017, 8:30AM), <https://www.lawfareblog.com/warning-about-tallinn-20-%E2%80%A6-whatever-it-says> (identifying the same issue with the data-as-object question contained in the Tallinn Manual).

217. TALLINN MANUAL 2.0, *supra* note 4, at 333.

218. *Id.* at 343.

219. *Id.*

220. *Id.* at 416.

221. See *Top 5 Things the Cloud is Not*, WIRED, <https://www.wired.com/insights/2012/06/top-5-things-the-cloud-is-not/> (last visited Mar. 14, 2021); TALLINN MANUAL 2.0, *supra* note 4, at 342.

222. See Wired, *supra* note 221.

highly movable and transferable state, data is somewhere.<sup>223</sup> Your term paper, your family photo, every individual's stock holdings, and the United States' nuclear launch codes are made up of millions of individual bits that are present on some data storage device, somewhere.<sup>224</sup> What destruction of data looks like is the rearrangement of those bits, making them unreadable and therefore unusable.<sup>225</sup> In a highly literal sense, this destruction is no different than the destruction of a building: the elemental building blocks are physically rearranged making them unrecognizable.<sup>226</sup> Likewise, when a missile hits its target, the underlying matter is not gone: its fundamental elements, made up of stone, bricks, and metal beams, are still there, but like the altered data, they are rearranged into an unusable state.<sup>227</sup> Data might not "go boom" in the same way, but it is still physically changed (i.e. destroyed).<sup>228</sup> Contrary to the Manual and the ICRC's claims, data and the underlying bits it is comprised of, are physical.<sup>229</sup>

One need not go down that literal path to still see the relevance of considering data as no different than physical objects.<sup>230</sup> Assuming, *arguendo* that data is not purely physical in the technical sense, it is still appropriate to not distinguish it from conventional objects or see a physical damage requirement for an armed attack.<sup>231</sup> First and foremost, doing so would involve returning to a means-based test, which would come to the illogical conclusion that rendering hardware on a single computer inoperable might constitute an armed attack, whereas destroying the data constituting a stock market without

---

223. *Id.*

224. *What are Bits, Bytes, and Other Units of Measure for Digital Information?*, IND. U., <https://kb.iu.edu/d/ackw> (last modified Jan. 18, 2018) [hereinafter *Measures for Digital Information*].

225. Chris Woodford, *Hard Drives*, EXPLAIN THAT STUFF, <https://www.explainthatstuff.com/harddrive.html> (last visited Aug. 13, 2020).

226. See Kayla Matthews, *What Role Does Data Destruction Play in Cybersecurity?*, MALWAREBYTES LABS (Jan. 7, 2020), <https://blog.malwarebytes.com/business-2/2019/09/what-role-does-data-destruction-play-in-cybersecurity/>.

227. *Id.*

228. Matthews, *supra* note 226.

229. PILLOU ET AL., *supra* note 209, at 633.

230. TALLINN MANUAL 2.0, *supra* note 4, at 342.

231. *Id.*

physical effect would not be considered an armed attack.<sup>232</sup> Article 52 of Additional Protocol I to the Genève Conventions of 1949 (API), and the ICRC's Commentary thereof,<sup>233</sup> while not directly on point for defining the scope of an armed attack, but reasonably relied on by the Tallinn Manual,<sup>234</sup> separated military and civilian objects from objectives.<sup>235</sup> Article 47 of the Draft Protocol contained, as recounted in the ICRC Commentary,<sup>236</sup> a non-exhaustive list of civilian objects, "such as houses, dwellings, installations and means of transport, and all objects which are not military objectives."<sup>237</sup> The intent of Article 52 of API was not to imply that non-physical objects could be attacked, but in 1977, one would have no conception of what attack upon a non-physical object could look like without physical effects.<sup>238</sup>

With this pre-digital lens in mind, it is no wonder that in the year 1500, the dominant maritime power of the day, and active rule-maker of customary international maritime law, the United Kingdom, would have seen a blockade as an act of war.<sup>239</sup> Also, why destruction or seizure of the Dutch spice fleet was so clearly a national threat to the Netherlands.<sup>240</sup> The mercantile fleets were the instruments of national power, commerce, communication, and empire;<sup>241</sup> centuries and countless advancements later, the internet has become this irreplaceable instrument for commerce and financial institutions today.<sup>242</sup> Further, with the development of precision guided munitions

---

232. *Id.* at 343.

233. PILLOUD ET AL., *supra* note 209, at 26.

234. TALLINN MANUAL 2.0, *supra* note 4, at 416.

235. Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and Relating to the Protection of Victims of International Armed Conflict (Protocol I) art. 52(1), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

236. PILLOUD ET AL., *supra* note 209, at 633.

237. *Id.*

238. Additional Protocol I, *supra* note 235, art. 52(1).

239. See generally Karl Zemanek, *Was Hugo Grotius Really in Favour of the Freedom of the Seas?*, 1 J. HIST. INT'L L. 48 (1999).

240. *Id.*; see also *A Taste of Adventure*, ECONOMIST (Dec. 17, 1998), <https://www.economist.com/unknown/1998/12/17/a-taste-of-adventure>.

241. Zemanek, *supra* note 239.

242. JAMES MANYIKA & CHARLES ROXBURGH, MCKINSEY GLOB. INST., THE GREAT TRANSFORMER: THE IMPACT OF THE INTERNET ON ECONOMIC GROWTH AND PROSPERITY 1–2 (2011), [https://www.mckinsey.com/~media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/The%20great%](https://www.mckinsey.com/~media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/The%20great%20transformer)

and the ability to conduct precise lower collateral death and injury bombing, while the law did not change, the reasonableness of efforts of distinction and proportionality may have.<sup>243</sup> With development of cyber weapons, the law should be no different. Would the destruction of the East India Company's annual trade on the docks of Portsmouth or the burning of all the stock certificates in New York or the forcible theft of all the gold in Fort Knox by another state be seen as an armed attack? The answer is clearly yes.<sup>244</sup> A pre-cyber thinker might not have been able to imagine a means of commerce, communication, logistics, and warfare that was more valuable in terms of money, power, and national importance than most physical objects. Nonetheless, children who have grown up never knowing the pre-internet world do not share this problem of being unable to see the "virtual" world as one-in-the-same as the physical world.<sup>245</sup> Is it any different for someone to take physical dollars from your pocket or drain your savings account, stealing your electronic dollars? No. When those of us that grew up before the internet are gone, perhaps even sooner, this notion of a distinction will seem quaint.<sup>246</sup>

Regardless of which approach one takes, one should end up in the same place, viewing data as an object.<sup>247</sup> While the first argument—that data is made up of bits that are physical things—might seem hyper-technical, the counterargument that an armed attack can only occur against physical objects is conversely hyper-technical, in the

---

20transformer/MGI\_Impact\_of\_Internet\_on\_economic\_growth.pdf.

243. Danielle L. Infeld, Note, *Precision-Guided Munitions Demonstrated Their Pinpoint Accuracy in Desert Storm; But is a Country Obligated to Use Precision Technology to Minimize Collateral Civilian Injury and Damage*, 26 GEO. WASH. J. INT'L L. & ECON. 109, 118–19 (1992).

244. While exceeding the scope of this writing, it is interesting to consider the question of whether to treat "ransomware," the act of holding data hostage, as digital damage or perhaps closer to blockade-like actions? See Sean D. Murphy, *Terrorism and the Concept of Armed Attack in Article 51 of the U.N. Charter*, 43 HARV. INT'L L.J. 41, 47–9 (2002) (arguing that acts of terrorism like the September 11 attack on the United States should be perceived as armed attacks, relying partially on the economic component).

245. See AARON SMITH, JANNA QUITNEY ANDERSON & LEE RAINIE, PEW RSCH. CTR., THE FUTURE OF MONEY: SMARTPHONE SWIPING IN THE MOBILE AGE (Apr. 17, 2012), <https://www.pewresearch.org/internet/2012/04/17/main-findings-the-future-of-money/>.

246. *Id.*

247. TALLIN MANUAL 2.0, *supra* note 4, at 343, 437.

extreme. Assumedly, the limited definition of an “object” from the ICRC’s Commentaries to the Additional Protocols was meant to exclude more ephemeral notions, such as people’s morale, ideals, love, joy, happiness, etc.<sup>248</sup> If that was the intent, then I agree, abstract notions cannot *per se* be considered objects that are attacked. But if attacks on the banks, telephone lines, letter carriers, stock trading floors of the past would constitute an attack, then there is no difference with their cyber equivalents.<sup>249</sup> Provided that data is an object, and purely digital damage alone could constitute an armed attack,<sup>250</sup> still does not answer the ultimate problem with the Scale and Effects School: where is the threshold between a simple use of force and an armed attack?<sup>251</sup>

Accepting *arguendo* again, that there is a gap between Articles 2(4) and 51, and the scale and effects test defines that gap, the totality of the “consequences”<sup>252</sup> should be considered in the differentiation. Admittedly, only economic means, without an underlying use of force, could never be violative of Article 2(4).<sup>253</sup> But, presumably, to the Court in *Nicaragua* one soldier firing across a border and striking a tree in another country would be a use of force, but not an armed attack.<sup>254</sup> Conversely, a missile strike that caused no deaths or injuries, yet knocked out an entire country’s or region’s telecommunication network would be an armed attack.<sup>255</sup> The consequences of the use of force make the difference.<sup>256</sup> But the Scale and Effects School struggles to draw this line clearly in the cyber domain.<sup>257</sup> First, as discussed, is the unreasonable size of the gap, as seen in the *Oil*

---

248. PILLOUD ET AL., *supra* note 209, at 633.

249. *Id.*

250. TALLIN MANUAL 2.0, *supra* note 4, at 342–43.

251. *Id.* at 332, 341.

252. *See* Netherlands Letter, *supra* note 101; *see also* Schmitt, *supra* note 204, at 911–12.

253. Schmitt, *supra* note 204, at 909 (“A temporary and spatially limited border incursion is probably a lesser threat to either international peace and security or the right of states to conduct their affairs free from outside interference than was the 1973–1974 Arab oil embargo.”).

254. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 228 (June 27).

255. *Id.* ¶ 191.

256. *Id.* ¶ 195.

257. TALLINN MANUAL 2.0, *supra* note 4, at 341.



*Platforms* case;<sup>258</sup> second, assuming the gap, the Tallinn Manual undervalues cyber damage.<sup>259</sup>

All cyber-attacks are not the same. But thinking about how various attacks cause harm is helpful to better classify how to think about them.<sup>260</sup> Analyzing the following three comparisons of conventional means, where there might be some agreement, may help unpack questions about how to conceive of the consequences: electronic jamming versus destroying communication networks; economic sanctions versus blockades; and espionage versus sabotage.<sup>261</sup>

There might be greater consensus that the former in each group would not constitute an armed attack, or potentially even use of force, whereas the latter of each dyad would.<sup>262</sup> Thus, when asking whether a cyber operation is more like the former or the latter, the answer also reveals whether a cyber operation likewise justifies or does not justify self-defense. The more closely the damage resembles that “resulting from the use of traditional weaponry is likely to be viewed as a use of force under Article 2(4);”<sup>263</sup> however, as cyber weapons become more commonplace, notions of what “traditional weaponry” is must be expanded.<sup>264</sup>

First, “A [cyber-attack] is often defined inadequately as disrupting, denying, degrading, or destroying either information resident in a computer network or the network itself.”<sup>265</sup> In reality, the use of

---

258. *Oil Platforms (Iran v. U.S.)*, Judgment, 2003 I.C.J. 161, ¶ 72 (Nov. 6) (separate opinion by Simma, J.).

259. TALLINN MANUAL 2.0, *supra* note 4, at 330.

260. See Silver, *supra* note 3, at 76–77 (providing a non-exhaustive list of four types of cyber operations, “(i) extracting the information held in the target computer (espionage); (ii) disseminating information through the adversary’s information network in order to deceive the adversary or stimulate political instability; (iii) preparing the battlespace by incapacitating the adversary’s command, control, and communication capabilities; (iv) causing property damage, physical injury, or death by manipulating infrastructure or operational systems controlled by the target computer.”).

261. See *id.* at 85.

262. TALLINN MANUAL 2.0, *supra* note 4, at 336.

263. Silver, *supra* note 3, at 85.

264. Int’l Comm. of the Red Cross Geneva, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*, 88 INT’L REV. OF THE RED CROSS 931, 937 (2006).

265. Dinstein, *supra* note 32, at 102.

electronic jamming or electronic warfare can take many forms.<sup>266</sup> The most common involves using electronic signatures to hide or disguise ships or aircraft.<sup>267</sup> It would also be possible to broadcast such wide radio frequencies to interrupt all forms of communication that use a radio frequency, thereby severely limiting a state's ability to communicate.<sup>268</sup> On the opposite side of this spectrum would be the actual physical destruction of telecommunication hubs, effectively stopping all electronic communication.<sup>269</sup> However, the Charter specifically cites, "[t]hese may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations," as not uses of force when employed by the Security Council.<sup>270</sup> While, the use of jamming or broadcasting into a state may very well be illegal, The UN Convention of the Law of Sea (UNCLOS), for example, makes unauthorized broadcasts from the high seas unlawful, going so far as to give jurisdiction for prosecution (among other states) to "any State where authorized radio communication is suffering interference."<sup>271</sup> If the duration is limited, and effects small, jamming might not even rise to the level of a use of force, whereas a missile strike upon communication hubs that cuts off all communication, destroys systems, and takes large efforts should

---

266. *See id.*

267. *See* Kris Osborn, *Revealed: The US Military's Electronic War Strategy to Counter Russia*, NAT'L INT. (Dec. 6, 2016), <https://nationalinterest.org/blog/the-buzz/revealed-the-us-militarys-electronic-war-strategy-counter-18644#:~:text=US%20MilitaryPolitics-,Revealed%3A%20The%20US%20Military's%20Electronic%20War%20Strategy%20to%20Counter%20Russia,electromagnetic%20spectrum%20to%20attack%20enemies>.

268. *See* John Keller, *DARPA Seeks to Ensure Radio Communications and Networking Reliability in Jamming and Interference*, MIL. & AEROSPACE ELECS. (Jan. 8, 2018), <https://www.militaryaerospace.com/computers/article/16726529/darpa-seeks-to-ensure-radio-communications-and-networking-reliability-in-jamming-and-interference>.

269. *See* Schmitt, *supra* note 204, at 888 (explaining the various ways that cyber-attacks are conducted).

270. U.N. Charter art. 41; *see also* Schmitt, *supra* note 204, at 912.

271. United Nations Convention on the Law of the Sea art. 109, Dec. 10, 1982, 1833 U.N.T.S. 397.

clearly be an armed attack.<sup>272</sup> For a cyber-operation that attacks communication systems, what are the effects or consequences? If the duration goes beyond the momentary, into the days, weeks, months; the effect is near total, such as preventing a government from being able to communicate within its system, as in Estonia in 2007, and/or the damage is permanent or takes large scale digital efforts to repair, then the cyber-operation tends to have consequences that are much closer to that of a missile strike on communications hubs and should likewise be considered an armed attack.<sup>273</sup>

Under the scale and effects test, since the means are (purportedly) unimportant, one must look only at the effects.<sup>274</sup> If the effects are essentially equal, the destruction of a communication system by physically destroying telephone wires or corrupting data to a point where the non-physical infrastructure would need to be “repaired” digitally, then both should constitute armed attacks.<sup>275</sup>

The second comparison is economic pressure versus a blockade.<sup>276</sup> Generally, economic pressures, such as sanctions, tariffs, and trade policy, are not viewed as force prohibited by Article 2(4).<sup>277</sup> “At the 1945 UN Charter drafting conference in San Francisco, States considered and rejected a proposal to include economic coercion as a use of force.”<sup>278</sup> Likewise, UN General Assembly Resolution 2625

---

272. See CHRISTINE GRAY, *INTERNATIONAL LAW AND THE USE OF FORCE* 107 (2000) (finding that acts of self-defense only warrant countermeasures that are proportional and necessary to respond to an armed attack).

273. See Dinstein, *supra* note 32, at 105 (finding that the outcome of a cyber-attack is more telling than the method used in order to justify self-defense).

274. See TALLINN MANUAL 2.0, *supra* note 4, at 340 (“[W]hether a cyber operation constitutes an armed attack depends on its scale and effects.”); *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996 I.C.J. 226, ¶ 72 (1996).

275. TALLINN MANUAL 2.0, *supra* note 4, at 340.

276. See discussion *infra* part I.

277. See Silver, *supra* note 3, at 80 (explaining that economic coercion is not considered a threat of force amongst scholars, yet the discourse is readily evolving); see also Schmitt, *supra* note 204, at 908 (“[T]he concept of the use of force is generally understood to mean armed force.”).

278. TALLINN MANUAL 2.0, *supra* note 4, at 331; 6 Documents of the United Nations Conference on International Organization 331, 334 U.N. Doc. 784 I/1/27 (June 5, 1945); 3 Documents of the United Nations Conference on International Organization 251, 252–53 U.N. Doc. 2 G/7(e)(4) (May 6, 1945).

rejected “all forms of pressure, including those of a political or economic character” as constituting force.<sup>279</sup> In contrast, a blockade has historically been seen a use of force by belligerents,<sup>280</sup> and certainly, if more than momentary, should be seen as an armed attack.<sup>281</sup> In UN General Assembly Resolution 3314, the Assembly, cited a “blockade of the ports or coasts of a State by the armed forces of another State” as an act of aggression.<sup>282</sup> The Statute of the International Criminal Court further includes blockade in its definition of the crime of aggression.<sup>283</sup> Further, “[a] majority of the [IGE] concluded that it is reasonable to apply the law of blockade to operations designed to block cyber communications.”<sup>284</sup> While the analogy to a blockade is imperfect, a blockade traditionally necessitates a threat of physical force in order to effectuate.<sup>285</sup> If cyber weapons are weapons, and a cyber-attack has occurred that effectually inhibits a state’s ability to conduct commerce, a cyber blockade is not a threat of force, but an effectuated use of force.<sup>286</sup> Therefore, while some would incorrectly see a blockade as “more forceful” because of the future threat of physical force, they would be incorrect, since a “cyber blockade” involves a completed use of force.<sup>287</sup>

There is a fundamental difference between a widespread, persistent denial of service attack, such as 2007 Estonia attack, and normal economic measures.<sup>288</sup> First, sanctions, tariffs, or adverse trade policy

---

279. TALLINN MANUAL 2.0, *supra* note 4, at 331.

280. See James F. McNulty, *Blockade: Evolution and Expectation*, 62 INT’L L. STUD. SER. US NAVAL WAR COLL. 172, 172 (1980) (noting that maritime blockades are internationally recognized as a lawful state action); see generally SAN REMO MANUAL, *supra* note 185, arts. 93–104 (detailing blockade guidelines in an attempt to modernize respective maritime naval discourse).

281. See *id.* arts. 93–104.

282. G.A. Res. 3314 (XXIX), art. 3(c) (Nov. 12, 1974).

283. Rome Statute of the International Criminal Court art. 8*bis* 2(c), July 17, 1998, 2187 U.N.T.S. 3.

284. TALLINN MANUAL 2.0, *supra* note 4, at 385, 505.

285. See Abram Chayes, *Law and the Quarantine of Cuba*, 41 FOREIGN AFFS. 550, 552 (1963) (“[T]he carriage of offensive weapons, against which it was directed, was something other than ordinary maritime commerce.”).

286. TALLINN MANUAL 2.0, *supra* note 4, at 329–30.

287. See RUSSELL, *supra* note 69, at 149 (finding that physical blockades share many of the same characteristics of cyber-attacks).

288. See *id.* (explaining how the 2007 cyber-attack on Estonia created widespread disruption on daily tasks conducted by the government and many private sector

are likely, absent treaty violation, lawful and not even a use of force.<sup>289</sup> On the other hand, even a short or partial blockade, in terms of location or type of goods, could rise to an armed attack.<sup>290</sup> For instance, Kennedy's month-long self-styled "quarantine" of Cuba, preventing only "offensive weapons," likely was an armed attack.<sup>291</sup> Israel used the Egyptian blockade of the Gulf of Aqaba in 1967 as one of actions justifying self-defense.<sup>292</sup> Again, to accept the position of the scale and effects test, were a cyber-attack that had the same scale and effects as a physical blockade that would rise to the level of an armed attack, then the cyber-attack should be viewed likewise an armed attack.<sup>293</sup>

An interesting, related scenario would be massive monetary counterfeiting, effectively devaluing another state's currency.<sup>294</sup> Counterfeiting would certainly be unlawful, as a violation of another state's sovereignty, but not a use of force.<sup>295</sup> While an unlikely, and highly particular, kind of cyber-attack, it is interesting to consider how to classify an attack that would put hundreds of thousands of dollars in to everyone's account, rather than making their accounts inaccessible—thus causing mass devaluation.<sup>296</sup> The digital damage

---

businesses).

289. See TALLINN MANUAL 2.0, *supra* note 4, at 331, 336 (describing how definitions of "threat of force" have evolved over time, yet prohibition of commerce with other states does not fit under the "threat of force" umbrella).

290. See generally SAN REMO MANUAL, *supra* note 185, arts. 93–104.

291. See Chayes, *supra* note 285, at 550 (equating the Kennedy administration's naval blockade of Cuba following their acquisition of Soviet missiles to an armed attack).

292. See THOMAS M. FRANCK, RECOURSE TO FORCE: STATE ACTION AGAINST THREATS AND ARMED ATTACKS 101–03 (2002) ("[I]t 'could of course, be argued that the Egyptian blockade itself constituted the use of force, thus legitimizing Israeli actions without the need for 'anticipatory' conceptions of self-defense.'").

293. See RUSSELL, *supra* note 69, at 62, 63 (stating that cyber-attacks share many of the same characteristics as physical blockades, yet do not justify the use of force as a response).

294. See Bruce G. Carruthers & Melike Arslan, *Sovereignty, Law, and Money: New Developments*, 15 ANN. REV. L. & SOC. SCI. 521, 527 (2019) (showing how counterfeiting an enemy nation's currency with the intention to destabilize its economy was largely ignored by international enforcement organizations prior to the twentieth century).

295. See *id.* at 521.

296. See Silver, *supra* note 3, at 82, 87 (finding that cyber-attacks have the potential to cripple target economies, and thus should be considered under the jurisdiction of Article 2(4) of the U.N. Charter).

done by forcing entry into the bank's security system might be enough to constitute force rising to an armed attack, but such an attack appears to be closer to counterfeiting than an armed attack.<sup>297</sup>

Ultimately, the quantity of commerce that is conducted over the internet and the scale of globalization only increase the consequences of closing another state off from the rest of the world.<sup>298</sup> Since the damage could be equivalent, if not greater, to a traditional blockade, thus raising the consequences, a modern "cyber blockade" should be considered an armed attack.<sup>299</sup>

Espionage versus sabotage is another interesting comparison. Like cyber-operations, state responsibility will always be in doubt with espionage and sabotage.<sup>300</sup> As provided in the American television program *Mission Impossible* "As always, should you or any of your IM Force be caught or killed, the Secretary will disavow any knowledge of your actions,"<sup>301</sup> governments will deny involvement when they get caught.<sup>302</sup> While the actual perpetrators of espionage are clearly committing domestic crimes, often under the cover of diplomatic immunity,<sup>303</sup> pure espionage is a generally and begrudgingly tolerated practice by most states,<sup>304</sup> and rarely seen as a use of force justifying self-defense.<sup>305</sup> Dinstein would classify espionage as "merely unfriendly acts."<sup>306</sup> Whereas pure espionage

---

297. *Id.*

298. See Dinstein, *supra* note 32, at 105 (explaining that the currently rising reliance on technology could expose State vulnerabilities to cyber-attacks).

299. *Id.*

300. See Asaf Lubin, *The Liberty to Spy*, 61 HARV. INT'L L. J. 185, 225 (2020) ([S]tates 'over-whelmingly refuse to admit responsibility for this conduct, let alone attempt to justify it as permissible under international law.'").

301. *Mission Impossible: Pilot* (CBS television broadcast Sep. 17, 1966).

302. See Lubin, *supra* note 300, at 225.

303. See generally Nathaniel P. Ward, *Espionage and the Forfeiture of Diplomatic Immunity*, 11 INT'L LAW. 657, 657–66 (1977) ("Such a denial of criminal immunity for espionage would subject the collector to domestic sanctions and serve as a deterrent against future abuses of privileges and immunities.").

304. *Id.*; see also Lubin, *supra* note 300, at 189 ("[S]tates enjoy a peacetime right to spy under international law.").

305. See Dinstein, *supra* note 32, at 105 (finding that acts of espionage generally do not rise to the level of an armed attack and are often openly recognized by a State).

306. *Id.*

should not be viewed as a use of force, and perhaps not even a violation of international law.<sup>307</sup> Sabotage, such as the act of an individual entering another country and destroying equipment or technology, certainly is more likely to be viewed as an unlawful use of force that justifies self-defense.<sup>308</sup> If an effects-based analysis is what matters, whether a factory is destroyed by sabotage or a missile, the outcome—a defunct factory—is the same net effect.<sup>309</sup> For espionage purposes, assume that a government used cyber means to infiltrate a computer system and steal state secrets in a second country; this is likely an unlawful act, but it does not appear to even rise to the level of a use of force.<sup>310</sup> Assume that, similar to the Stuxnet operation,<sup>311</sup> a government infiltrated a computer system to destroy another state's capability to make a certain weapon system; this act, like conventional sabotage, is certainly a use of force and would produce effects that should be considered an armed attack.<sup>312</sup>

## VIII. PRESCRIPTIVE PROBLEMS

Despite the Tallinn Manual explicitly limiting itself to a descriptive analysis,<sup>313</sup> a question that must be considered remains: is the scale and

---

307. See *id.* at 101 (finding that merely unfriendly acts—such as espionage—does not trigger countermeasures in any accepted norm of international law); see also *Episode 158: What SCOTUS Can Learn from Franklin Barbecue*, NAT'L SEC. L. PODCAST, at 32:00 (Mar. 11, 2020), <https://www.nationalsecuritylawpodcast.com/episode-158-what-scotus-can-learn-from-franklin-barbecue/> (stating that U.S. Department of Defense does not consider military cyber-attacks as a violation of international law—much like espionage).

308. Silver, *supra* note 3, at 87, 88; see generally *Ex Parte Quirin*, 317 U.S. 1, 18–37 (1942) (holding that acts of sabotage and physical destruction of American war industries by German Reich spies is a violation of international law).

309. See Dinstein, *supra* note 32, at 102–03 (“The crux of the matter is not the medium at hand . . . but the violent consequences of the action taken.”).

310. TALLINN MANUAL 2.0, *supra* note 4, at 335.

311. See Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things*, 72 UNIV. MIA. L. REV. 761, 787, 789 (2018) (explaining that Stuxnet was a sophisticated computer virus aimed to disrupt Iranian development of nuclear weapons).

312. TALLINN MANUAL 2.0, *supra* note 4, at 336, 415; Dinstein, *supra* note 32, at 101.

313. See *id.* at 2–4 (explaining that the Tallinn Manual is presented by international law experts as commentary on the law as it exists).

effects test, as applied, desirable? The answer is clearly no.<sup>314</sup> As the Charter-is-Dead School accurately confronts, the Security Council system for dealing with unlawful uses of force is likely irretrievably broken.<sup>315</sup> Complaining to the UNSC is unlikely to produce an acceptable result for states that are victims of conventional or cyber force.<sup>316</sup> The Scale and Effects School would leave an unacceptable gap constituting unlawful force short of an armed attack that would not allow states to use force, even as the only available means to defend themselves.<sup>317</sup> Whatever one makes of the confusing language in Article 51 – “Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations . . .”<sup>318</sup> – it cannot mean that states are left without the ability to exercise self-defense in response to unlawful force.

This interpretation, as the Scale and Effects School would advance, makes most states lawbreakers, only further tilting the world toward the Charter-is-Dead School.<sup>319</sup> Assumedly, however, proponents of the scale and effects test still believe that this is or should be the law governing the use of force.<sup>320</sup> The only way one can reconcile the logic of the Court in *Nicaragua* is by having a belief that the Court’s framing would produce less force not more, a laudable objective.<sup>321</sup> While the judgment of the court might have some deterrent effect on some states to refrain from using force in self-defense, it has the opposite effect on aggressor states (the very states we should worry about) that would choose to use force, albeit short of an armed attack, more often.<sup>322</sup> This effect is only truer in the cyber domain.<sup>323</sup> Applying the Tallinn

---

314. *Id.*

315. *Id.* at 330–31; *Oil Platforms (Iran v. U.S.)*, Judgment, 2003 I.C.J. 161, ¶ 6 (Nov. 6) (separate opinion by Simma, J.).

316. See TALLINN MANUAL 2.0, *supra* note 4, at 330–31.

317. *Id.*

318. UN Charter, art. 51.

319. See generally FRANCK, *supra* note 292, at 53–68 (explaining how terrorism is an excellent predictor of both how states will respond to cyber-attacks and the incredible difficulty in assigning blame).

320. See TALLINN MANUAL 2.0, *supra* note 4, at 333 (stating that the *Nicaragua* judgment founded the scale-and-effects test).

321. See generally FRANCK, *supra* note 292, at 53–68.

322. *Id.* at 62.

323. See Davis, *supra* note 29.



Manual's framing might make some states less likely to use force in self-defense against cyber operations, thereby incentivizing aggressor states to use cyber means short of an armed attack, without the fear of conventional force in response, especially if the aggressor state is a permanent member of the UNSC.<sup>324</sup> "Lawfare" would also incentivize starting conflicts in the cyber domain, because while the aggressor state might be called a lawbreaker, if the aggressor could goad the victim into responding with force, physical or cyber, it would make lawbreakers of both parties.<sup>325</sup>

So-called "pin-prick" or "accumulation of events" attacks highlight this problem.<sup>326</sup> "Pin prick" attacks would be a "series of cyber incidents that individually fall below the threshold of an armed attack."<sup>327</sup> The Tallinn Manual, correctly, would generally treat "the incidents as a composite armed attack," i.e., judged collectively.<sup>328</sup> But the idea of pin prick attacks raises an interesting question: Under the extremely high scale and effects test, what if there is a long, continuous use of relatively minor attacks that never rise to an armed attack? Under the Scale and Effects School, this would conceptually allow aggressor states to perpetually pick away at another state forever, without the fear of recourse.<sup>329</sup>

As shown, the scale and effects test struggles in every way to discuss the law: predictively, descriptively, and prescriptively.<sup>330</sup> Despite being the dominate view, it does not reflect how states will behave, what the law is, or what it should be.<sup>331</sup> The School does attempt to deal with clear drafting and interpretation problems of the

---

324. TALLINN MANUAL 2.0, *supra* note 4, at 330–31.

325. *Id.*

326. See GRAY, *supra* note 132, at 107 (explaining how a single use of force may not warrant lawful countermeasures, however, a series of collective uses of force may amount to an armed attack deserving of self-defense).

327. TALLINN MANUAL 2.0, *supra* note 4, at 342; Dinstein, *supra* note 32, at 109.

328. TALLINN MANUAL 2.0, *supra* note 4, at 342.

329. Dinstein, *supra* note 32, at 109.

330. TALLINN MANUAL 2.0, *supra* note 4, at 342.

331. See Papawadee Tanodomdej, *The Tallinn Manuals and the Making of the International Law on Cyber Operations*, 13 MASARYK U. J. L. & TECH. 67, 82 (2019) (discussing the challenges of certain pedagogical debates in international law).

UN Charter,<sup>332</sup> but the solution advanced by the Court in *Nicaragua*, adopted by the Tallinn Manual, and made into government policy by the Netherlands fails to be an accurate or workable description of the law of self-defense.<sup>333</sup>

## IX. FORCEFUL COUNTERMEASURES SCHOOL

The Forceful Countermeasures School is an attempt to deal with many of the criticisms of the Scale and Effects School.<sup>334</sup> Fundamentally, this School starts with the same interpretation of the language and gap created by Articles 2(4) and 51 of the UN Charter, specifically the differentiation between the terms “use of force” and “armed attack” that all armed attacks consist of uses of force, but not every use of force rises to the level of an armed attack.<sup>335</sup> Similarly, many from this School would adopt the scale and effects test from *Nicaragua*.<sup>336</sup> Unlike the Scale and Effects School, as I have defined it, the Forceful Countermeasures School would see the use of forceful countermeasures, in response to unlawful uses of force, as lawful.<sup>337</sup>

Countermeasures, generally, would be any act (forceful or not) that would on its own be unlawful, but are permissible in response to an unlawful act, in an attempt to return an aggressor state to lawful

---

332. See *id.* (describing the imbalance and questionable authority as a result of “opaque drafting processes” that leads to disharmony within the school of thought).

333. See Michael Sang, Legal Regulation of Cyber Warfare: Reviewing the Contribution of the Tallinn Manual to the Advancement of International Law 48 (Feb. 2015) (M.A. Thesis, Univ. of Cape Town) (on file with OpenUCT), [https://open.uct.ac.za/bitstream/handle/11427/15201/thesis\\_law\\_2015\\_sang\\_michael\\_kipkemei.pdf?sequence=1&isAllowed=y](https://open.uct.ac.za/bitstream/handle/11427/15201/thesis_law_2015_sang_michael_kipkemei.pdf?sequence=1&isAllowed=y) (stating that there is a general lack of clarity in the Tallinn Manual to explain how states can respond to cyber-attacks, which ultimately “diminishes its practical utility”).

334. See Oona A. Hathaway, *The Drawbacks and Dangers of Active Defense*, 6 INT’L. CONF. CYBER CONFLICT 39, 44 (2014) (explaining how multiple terms in the U.N. Charter have different interpretations by different legal institutions in international law).

335. See *id.* (defining the solution set forth in *Nicaragua* as requiring “justified armed attacks under Article 51” to be only in response to those initial attacks that constitute the “most grave forms of the use of force”).

336. See *id.* at 45 (arguing that the Forceful Countermeasures school of thought is increasingly popular for cyber warfare).

337. See Dinstein, *supra* note 32, at 107 (describing an example of an armed attack in cyber warfare).

behavior.<sup>338</sup> The real split between the Scale and Effects School and the Forceful Countermeasures School is not whether countermeasures writ large are lawful, but whether countermeasures may involve force.<sup>339</sup> For example, a majority of the IGE agree that generally countermeasures could be applied in response to cyber uses of force, but only a minority would see a *forceful* countermeasure as lawful.<sup>340</sup>

Confusingly, the court in *Nicaragua* while setting a surprisingly high bar for when self-defense would be permissible, seems to hold out the possibility of forceful countermeasures: “analogous to the right of collective self-defence in the case of an armed attack, but both the act which gives rise to the reaction, and that reaction itself, would in principle be less grave.”<sup>341</sup> A relevant difference is that there would not be lawful collective countermeasures: there is not “the right of a third State to resort to force in response to the wrongful act.”<sup>342</sup> Although there is support for countermeasures even within the *Nicaragua* judgment,<sup>343</sup> the judgment itself is unclear if they would only be limited, non-forceful countermeasures.<sup>344</sup> Judge Simma

---

338. See *id.* (explaining how when an armed attack occurs, it is perfectly legitimate for a state to take action in the name of self-defense).

339. See TALLINN MANUAL 2.0, *supra* note 4, at 339 (distinguishing between an armed attack and aggression, whereby aggression does not always constitute an armed attack, and therefore, does not entitle a state to a forceful countermeasure); see also Claus Kreß, *The International Court of Justice and the ‘Principle of Non-Use of Force’*, in THE OXFORD HANDBOOK OF THE USE OF FORCE IN INTERNATIONAL LAW 561, 562–63 (Marc Weller ed., 2017) (providing an early example of when the ICJ considered international law and the use of force in the *Corfu Channel* case); YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 199 (3rd ed., 2004) (explaining how forcible countermeasures are unlawful if they are taken by a state in response to an action that never constituted an armed attack).

340. See TALLINN MANUAL 2.0, *supra* note 4, at 125 (“A minority of the Experts asserted that forcible countermeasures are appropriate in response to a wrongful use of force. . .”).

341. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 210 (June 27).

342. DINSTEIN, *supra* note 339, at 175.

343. See *Military and Paramilitary Activities*, 1986 I.C.J., ¶ 224.

344. See *id.*; see also Hargrove, *supra* note 49, at 138 (“The Court strongly suggested, but so far as I can ascertain did not explicitly assert, that the victim state’s ‘proportional countermeasures’ might themselves include the use of force.”); Hargrove, *supra* note 49, at 135, 141–42 (“Either the Court was saying (a) that there are some acts of force that nobody, not even the victim may resist by proportionate measures of force; or it was saying (b) that only the victim may resist by force,

provides the most articulate definition of forceful countermeasures in his separate opinion in *Oil Platforms*, using proportionality as the throttle for forceful responses:

To sum up my view on the use of force/self-defence aspects of the present case, there are two levels to be distinguished: there is, first, the level of “armed attacks” in the substantial, massive sense of amounting to “une agression armée”, to quote the French authentic text of Article 51. Against such armed attacks, self-defence in its not infinite, but still considerable, variety would be justified. But we may encounter also a lower level of hostile military action, not reaching the threshold of an “armed attack” within the meaning of Article 51 of the United Nations Charter. Against such hostile acts, a State may of course defend itself, but only within a more limited range and quality of responses (the main difference being that the possibility of collective self-defence does not arise, cf. *Nicaragua*) and bound to necessity, proportionality and immediacy in time in a particularly strict way.<sup>345</sup>

Looking only prescriptively, the incredibly high threshold for armed attack laid out by the Court appears much more reasonable if forceful countermeasures would be lawful.<sup>346</sup> This may have been the Court attempting to engage in regulating the very grey zone they created.<sup>347</sup>

The obvious textual problem with this explanation is that while the Court is slavishly particular to the language of Article 51’s “armed attack” threshold,<sup>348</sup> there is no textual support for countermeasures,

---

provided it did so alone. . . . In either case above, the Court would cripple the right of self-defense the more so in the former than the latter. But in the latter case, it would in one remarkable stroke manage both to impair the right of self-defense, and to weaken fundamentally the *prohibition* on the use of force by creating an open-ended and wholly new category of exception to Article 2(4).”).

345. See *Oil Platforms* (Iran v. U.S.), 2003 I.C.J. 161, ¶ 13 (Nov. 6) (separate opinion by Simma, J.).

346. See Abraham D. Sofaer, Legal Advisor, U.S. Dep’t of State, Luncheon Address at the American Society of International Law 82nd Annual Meeting 420, 426 (Apr. 22, 1988) (asserting that the court in *Nicaragua* did not consider necessity and proportionality in its reasoning, which contributed to the illegality of the forceful countermeasure).

347. *Oil Platforms*, 2003 I.C.J. 161, ¶ 6.

348. See William C. Banks & Evan J. Criddle, *Customary Constraints on the Use of Force: Article 51 with an American Accent*, 29 LEIDEN J. INT’L L. 67, 67 (2016) (explaining that permitting states to “use force only after another state has launched an ‘armed attack’ of sufficient magnitude to satisfy the event threshold requirement

forceful or otherwise.<sup>349</sup> The sections of the opinion dealing with countermeasures take the Court even further from the text of the Charter, effectively creating a “quadruple structure of (i) self-defense versus (ii) armed attack, and (iii) counter-measures analogous to but short of self-defense versus (iv) forceable measures short of an armed attack.”<sup>350</sup>

Predictively, lawful, forceful countermeasures would alleviate some of the problems the unrealistically high threshold Scale and Effects School creates, as forceful countermeasures at least give states a means to attempt to defend themselves.<sup>351</sup> However, a victim state is more likely to claim (and view) a use of force as an armed attack and respond with force equivalent to self-defense.<sup>352</sup> While Forceful Countermeasures has some predictive value over the Scale and Effects School, it is limited at best.<sup>353</sup>

Descriptively, this School, like the Court in *Nicaragua* struggles.<sup>354</sup> Without any direct textual authorization contained within the Charter, the Forceful Countermeasures School would rely on “nothing . . . shall impair” the “inherent right” of “self-defense” from Article 51, effectively retaining the pre-Charter right of Self-Help, allowing the use of force called an “armed reprisal.”<sup>355</sup> “Reprisals constitute ‘counter-measures that would be illegal if not for the prior illegal act

---

for responsible military action” is a ‘restrictive’ approach to self-defense).

349. See Hargrove, *supra* note 49, at 142 (“This new exception to Article 2(4)—‘forcible countermeasures’—is perhaps only the most obvious specific consequence of the Court’s treatment of customary law as the law of the case.”).

350. DINSTEIN, *supra* note 339, at 174.

351. See Hathaway, *supra* note 336, at 48 (referencing Judge Simma in *Oil Platforms*, who acknowledged that forceful countermeasures gave states the opportunity to defend themselves).

352. See Catherine Lotrionte, *State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, 26 EMORY INT’L L. REV. 861, 864 (2012) (arguing that certain cyber operations clear the “requisite level of harm” to constitute an armed attack and give a state legal leeway to take self-defense measures).

353. See Hathaway, *supra* note 336, at 50 (concluding that it would be unrealistic to make an all-out prohibition on a state using forceful countermeasures in response to a cyber-attack).

354. See *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 177 (June 27) (dissenting opinion by Schwebel, J.).

355. See *id.* ¶ 176.

of the State against which they are directed.”<sup>356</sup> This doctrine of reprisals pre-dates the supposed blanket ban on the use of the force in Article 2(4).<sup>357</sup> However, importantly, before the UN Charter, or at least the *Kellogg-Briand Pact*<sup>358</sup> there was no general ban on the use of force,<sup>359</sup> so it is hard to see how a right to forceful self-help would have intentionally survived the purported plain meaning of the Charter.<sup>360</sup> Considering the language of Article 51,<sup>361</sup> it is even harder to imagine the Charter limiting the right of self-defense as the Court in *Nicaragua* would,<sup>362</sup> while permitting an unmentioned exception to the quite specific prohibition on the use of force in Article 2(4).<sup>363</sup> Despite the language of the Court,<sup>364</sup> and assuming a bias of the Court against the use of force, it is hard to imagine the Court intended to imply that forceful countermeasures are lawful, as doing so would seem to close one door to the use of force while opening another.<sup>365</sup>

Alternatively, there may be space in the Forceful Countermeasures School for what could be called weak-hearted Charter-Is-Dead scholars, basically those who see significant state practice having eroded much of the Charter’s language, but still seek to retain some of its structure.<sup>366</sup> One such structural element is how “it appears that

356. DINSTEIN, *supra* note 339, at 194, quoting O. Schachter, *International Law Theory and Practice*, 178 R.C.A.D.I. 9, 168 (1982).

357. See MICHAEL WALZER, *JUST AND UNJUST WARS: A MORAL ARGUMENT WITH HISTORICAL ILLUSTRATIONS* 220 (1977) (explaining how the doctrine of reprisals will not be thoroughly considered, and that while the lawfulness of reprisals is dubious, it is still distinct from countermeasures as a reprisal is meant to punish).

358. See General Treaty for Renunciation of War as an Instrument of National Policy art. I–II, Aug. 27, 1928, 46 Stat. 2343, 94 L.N.T.S. 57 (entered into force Jul. 24, 1929) [hereinafter *Kellogg-Briand Pact*] (“The High Contracting Parties agree that the settlement or solution of all disputes or conflicts of whatever nature or of whatever origin they may be, which may arise among them, shall never be sought except by pacific means.”).

359. See *id.* (calling for an outright ban on the use of force to settle a dispute).

360. See DINSTEIN, *supra* note 339, at 194 (concluding that reprisal’s constitute illegal behavior made legal only because of a prior illegal act of a state).

361. See *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 176 (June 27).

362. See *id.* ¶ 193.

363. U.N. Charter art. 2, ¶ 4.

364. See *Nicaragua*, 1986 I.C.J., ¶¶ 224, 248–49.

365. See *id.*

366. See Robert J. Delahunty, *Paper Charter: Self-Defense and the Failure of the United Nations Collective Security System*, 56 CATH. U. L. REV. 871, 945 (2007)

recourse to self-help remains an option not entirely foreclosed by the Charter, at least as interpreted by state practice.”<sup>367</sup> The problem, again, with this analysis is that states employing reprisals of this nature, especially against a use of force long since concluded, unusually “resort to creative fictions” of self-defense.<sup>368</sup> Frequently, the international community has failed to object to these reprisals, when there is a sympathetically aggrieved party,<sup>369</sup> “lend[ing] further credence to the thesis that state recourse to force may be tolerated . . . even when the injury does not rise to the threshold of a ‘armed attack.’”<sup>370</sup> The U.S. response in Libya to the German nightclub bombing in 1986 is a perfect example of responding with force in claimed self-defense after the incident justifying self-defense has ceased.<sup>371</sup>

Countermeasures may not be as helpful as some would advance. Importantly, like self-defense (excluding arguments over the use of preemptive self-defense), countermeasures cannot be reprisals,<sup>372</sup> i.e., punishment for past actions, but instead efforts to return the aggressor state to lawful compliance. Dinstein would construe the concept of immediacy “broadly,” arguing “self-defense countermeasures must

---

(explaining that under the “Charter is dead” school of theory, because the international community continues to ignore the Charter’s rules, the Charter’s use of force rules are subsequently not binding).

367. FRANCK, *supra* note 292, at 112.

368. *Id.*

369. *Id.*

370. *Id.*; see also Anthony Clark Arend, *International Law and the Recourse to Force: A Shift in Paradigms*, 27 STAN. J. INT’L. L. 1, 14 (1990) (describing a “growing willingness to use force in certain ‘just’ circumstances” that might not meet the requisite threshold).

371. See Jeffrey Allen McCredie, *The April 14, 1986 Bombing of Libya: Act of Self-Defense or Reprisal?*, 19 CASE W. RES. J. INT’L. L. 215, 216 (1987) (providing an example of the United States making known its intent to use force in response to the Berlin nightclub bombing, despite the fact that there was no continuance of threat from the opposing state parties).

372. But see WALZER, *supra* note 357, at 220 (“Nor is there any evidence that individual members of the UN, however they vote on ritual occasions, are prepared to renounce reprisals when lives of their own citizens are at stake. Reprisals are clearly sanctioned by practice of nations, and the (moral) reason behind the practice seems as strong as ever.”).

not be too tardy,”<sup>373</sup> but he would permit them later than most.<sup>374</sup>

The “pin-prick” scenario is again helpful to consider in the forceful countermeasure context.<sup>375</sup> Assume different series of cyber-attacks that are possibly: a) completed, but do not collectively amount to an armed attack, b) completed, but none of the attacks *individually* would constitute an armed attack, assuming that aggregation of pin-prick attacks is not permitted, or c) ongoing. Only in category c) would countermeasures, forceful or not, be authorized.<sup>376</sup> But even if authorized, any action would still be shaped by the fundamental threshold question of what level of countermeasure force would be proportional to return the aggressor state to law compliance.<sup>377</sup>

As a descriptive matter, assuming the language of the Charter is still good law, it seems much more defensible that Article 2(4) eliminated forceful countermeasures, regardless of how one views whatever remains of self-defense.<sup>378</sup>

Prescriptively, Forceful Countermeasures might at first glance seem preferable to the Scale and Effects School, in that, at least, forceful countermeasures would act as a gap-filler to defend against unlawful force less than an armed attack;<sup>379</sup> however, a disjointed, messy system is all that would remain, and in the cyber domain, all the more so.<sup>380</sup>

---

373. Dinstein, *supra* note 32, at 110.

374. *Id.*

375. See Abhimanyu George Jain, *Rationalising International Law Rules on Self-Defence: The Pin-Prick Doctrine*, 14 CHI-KENT J. INT’L & COMPAR. L. 23, 27 (2014) (“The defensive use of force in this sort of situation may be justified by reference to the ‘pin-prick’ or ‘accumulation of events’ doctrine. This doctrine recognizes the existence of a right of self-defense in response to a series of armed attacks, each possibly falling below the gravity threshold, but together, constituting a continuing armed attack. . .”).

376. See *id.* at 58 (arguing that the court in the *Nicaragua* decision “implicitly allowed for the possibility of the pin-prick doctrine”).

377. See *id.* at 64 (explaining that under the pin-prick doctrine, “the necessity and proportionality analysis, as well as the gravity analysis, remain the same.”).

378. See Mary Ellen O’Connell, *Enforcing the Prohibition on the Use of Force: The U.N.’s Response to Iraq’s Invasion of Kuwait*, 15 S. ILL. U. L. J. 453, 457 (1991) (supporting the notion that the Charter is still good law because it has altered how governments decide to use force for the past one-hundred years).

379. See *id.* (explaining how when states use force today, they try to put forth a legal explanation).

380. See Matthew Bey, *Great Powers in Cyberspace: The Strategic Drivers Behind US, Chinese and Russian Competition*, 3 CYBER DEF. REV. 31, 31 (2018)



Under the scale and effects test, the question remains regarding the threshold of what constitutes an armed attack, a point even the Manual and the Netherlands struggled to define,<sup>381</sup> and states would continue to violate, while claiming compliance as self-help.<sup>382</sup> Forceful countermeasures would *also* create a second undefined threshold question of force “‘analogous’ to but less grave than self-defense.”<sup>383</sup> As Dinstein laid out in his “quadruple structure,” forceful countermeasures in response to unlawful force not rising to an armed attack could not rise to the level of self-defense.<sup>384</sup> As discussed, there cannot be self-defense in response to self-defense: someone must have “started it.”<sup>385</sup>

Imagine that Estonia could have stopped the 2007 attack with a so called “hack-back,” only destroying the computer responsible.<sup>386</sup> Would that be a lawful countermeasure? Presumably so.<sup>387</sup> But what if Estonia could only stop it with a single missile strike to the building housing the computer controlling the attack? Presumably, that would be a self-defense scale of a response.<sup>388</sup> What would be Russia’s lawful

---

(describing how the next frontier of critical battlegrounds is cyber warfare and that the process of developing international norms and treaties will inevitably be “messy”).

381. See Franck, *supra* note 10, at 816 (arguing that the Charter provides no answer for determining whether or not there has been an “armed attack”).

382. See *id.* (asserting that state practice has destroyed global confidence in Article 2(4) because of continuous violations).

383. DINSTEIN, *supra* note 339, at 174.

384. *Id.*

385. See Kretzmer, *supra* note 78, at 237–38 (acknowledging that there are pedagogical differences for defining what “just war” is).

386. See Samuli Haataja, *The 2007 Cyber Attacks Against Estonia and International Law on the Use of Force: An Informational Approach*, 9 L., INNOVATION & TECH. 159, 159–60 (2017) (“In April and May of 2007 Estonia had become subject to a new form of ‘cyber violence.’ It became the first nation-state subject to large-scale distributed denial of service (DDoS) attacks in what was widely described in the media as a ‘cyber war’ and what Estonia’s President later depicted as ‘Web War One.’”).

387. See Delbert Tran, Note, *The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack*, 20 YALE J. L. & TECH. 376, 399 (2018) (outlining potential responses a state party can take in response to a cyber-attack).

388. See *id.* (describing the possible responses to a cyber-attack to include (1) “negative economic punishment,” (2) “deni[al] of positive benefits” to the state responsible for the attack, (3) “hack-back countermeasure[s],” (4) “military response”).

response if Estonia, in taking a “countermeasure” then escalates the violence up to what should be considered self-defense, and therefore to the level of an armed attack? There can be no self-defense to a lawful action of self-defense, but can there be self-defense in response to an excessive countermeasure? This all seems better resolved by proportionality rather than a quadruple subjective structure.<sup>389</sup>

It is possible that the more complex scheme, with multiple thresholds, could have something of a circuit breaker effect, stopping escalation at each threshold.<sup>390</sup> But states disregarding and engaging “creative fictions” of both the aggressive force and counterforce seem more likely. As one can easily see, allowing the use of force below self-defense only obfuscates the analysis. If law is to have any regulatory effect on state behavior, the impact must be clear and have some connection to reality.<sup>391</sup> If the desired end state of the Charter is the following:

[T]o maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law,<sup>392</sup>

then forceful countermeasures work against this goal, not toward it.<sup>393</sup>

The Forceful Countermeasures School is rooted in a noble goal—the attempt to limit escalation of interstate violence, while providing credible remedies to victims of force<sup>394</sup>—but creates a messy, more

---

389. See DINSTEIN, *supra* note 339, at 174 (“What emerges is a quadruple structure of (i) self-defense versus (ii) armed attack, and (iii) counter-measures analogous to but short of self-defense versus (iv) forcible measures short of an armed attack.”).

390. See *id.* (referencing the “quadruple structure”).

391. See FRANCK, *supra* note 292, at 112 (describing some of the longstanding problems with use of force that can contribute to escalation of violence).

392. U.N. Charter art. 1, ¶ 1.

393. See 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) (stating that possible restraint on escalation during the use of force are found in the United Nation’s Security Council and international law’s “principle of the right to self-defense”).

394. See Jacqueline Van De Velde, *The Dangers of Forceful Countermeasures as a Response to Cyber Election Interference*, in DEFENDING DEMOCRACIES:

violent world.<sup>395</sup> This messy solution occurs for two reasons: first, by increasing the risk of force less than an armed attack, without the possibility of victim states to respond with self-defense, and second, without any support from the language of the Charter, authorizing states to use force in the form of countermeasures.<sup>396</sup>

## X. NO GAP SCHOOL

Rather than parsing the differences between the terms “use of force” from Article 2(4) and “armed attack” from Article 51, the No Gap School would argue that, effectively, there is no difference.<sup>397</sup> Adherents of this position focus on the “nothing . . . shall impair” and “inherent right” from the first phrase of Article 51: “[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs. . . .”<sup>398</sup> By this reading, there is a pre-Charter customary right of self-defense that the Charter does not extinguish.<sup>399</sup> “As the Charter’s drafting history makes clear, ‘[t]he use of arms in legitimate self-defense remains admitted and unimpaired.’”<sup>400</sup> Thus, the need “to distinguish ‘the most grave forms of the use of force (those constituting an armed attack) from other less grave forms’”<sup>401</sup> is eliminated.<sup>402</sup> Any use of force (presumably, unlawful force), therefore, authorizes a lawful use of force in response as self-defense.<sup>403</sup> This is certainly a minority

---

COMBATING FOREIGN ELECTION INTERFERENCE IN A DIGITAL AGE 215, 234 (Jens David Ohlin & Duncan B. Hollis eds., 2017) (arguing that “embracing the doctrine of forceful countermeasures would give states additional opportunities to escalate violence as a permissible option” rather than have escalation checks).

395. See Bey, *supra* note 380, at 31 (noting that cyberspace is a new environment, which means that the governing norms and treaties are not “universally accepted”).

396. See Kretzmer, *supra* note 78, at 275–76 (providing an example of how states construct a personal narrative that justifies and often escalates the use of force).

397. See Sofaer, *supra* note 346, at 425 (explaining that there is a basic reality in international law that states inherently have a right to self-defense).

398. U.N. Charter art. 51.

399. See *id.*

400. See Taft, *Self-Defense*, *supra* note 174, at 298 (furthering the idea that the use of arms in self-defense is a reality of international law).

401. Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶ 51 (Nov. 6) (separate opinion by Simma, J.).

402. *Id.*

403. OFF. GEN. COUNS., DEP’T DEF., DEP’T OF DEF. L. OF WAR MANUAL §16.3.3, 1016–17,

opinion in comparison to the more widely accepted Scale and Effects School,<sup>404</sup> however, “[t]he United States has long taken the position that the inherent right of self-defense potentially applies against any illegal use of force. Thus, any cyber operation that constitutes an illegal use of force against a State potentially gives rise to a right to take necessary and proportionate action in self-defense.”<sup>405</sup>

The No Gap School certainly proposes a neater rule than subjectively looking at the “scale and effects” and trying to determine when an operation crosses the “armed attack” threshold, which, then and only then, authorizes self-defense.<sup>406</sup> Thinking only textually, the text of Article 51 confuses its purpose.<sup>407</sup> First, why use different words (“use of force” versus “armed attack”)<sup>408</sup> in the different articles, if the drafters intended them to be equal?<sup>409</sup> Second, even if there is a pre-Charter right to self-defense, is it wholly unimpaired? Or is only the portion of the pre-Charter right that remains after an armed attack occurs?

One possible answer is that the difference in language is a simple error, “an inept piece of draftsmanship.”<sup>410</sup> This is certainly possible. Admittedly, despite the best efforts by drafters of any legal document to divine future disagreements, whether in contracts, statute, or

---

<https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190> (limiting U.S. self-defensive responses to cyber-attacks to cyber-attacks that constitute armed attack or imminent threat under U.N. Charter Art. 51) [hereinafter DOD LAW OF WAR MANUAL].

404. See Michael J. Glennon, *How War Left Law Behind*, N.Y. TIMES (Nov. 21, 2002), <https://www.nytimes.com/2002/11/21/opinion/how-war-left-the-law-behind.html> (Discussing the Scale and Effects school of thought).

405. See DOD LAW OF WAR MANUAL, *supra* note 403, §16.3.3.1, 1017, (further clarifying U.S. self-defensive responses to cyber-attacks to cyber-attacks that constitute armed attack under U.N. Charter Art. 51).

406. See Sofaer, *supra* note 346, at 425.

407. See JAMES A. GREEN, THE INTERNATIONAL COURT OF JUSTICE AND SELF-DEFENCE IN INTERNATIONAL LAW 114 (2009) (applying the term strategically rather than merely textually).

408. See U.N. Charter art. 2, ¶ 4 (differentiating “armed attack” from “use of force”); see U.N. Charter art. 51 (asserting member states’ right to use self-defense).

409. *Id.* arts. 2, ¶¶ 4, 51.

410. See DIMITRIOS DELIBASIS, THE RIGHT TO NATIONAL SELF-DEFENSE IN INFORMATION WARFARE OPERATIONS 131 (2007) (articulating the elements of an armed attack).

treaties, rarely are these documents given the same level of scrutiny in drafting as skilled litigants, juris, and scholars do after the fact to serve the best interests of their clients, desired outcome, or school of thought.<sup>411</sup> Another possibility is that the difference was not unintended; perhaps it was made in an effort to demonstrate the wide scope of self-defense, only to inadvertently imply a narrowing instead.<sup>412</sup> Certainly “aggression,”<sup>413</sup> also from Article 2(4), undiscussed here, conjures the German invasion of Poland, whereas “armed attack”<sup>414</sup> might be exactly what the Court in *Nicaragua* called a “mere frontier incident,”<sup>415</sup> i.e. violence done with arms.<sup>416</sup> This reading would invert the Court’s logic, allowing self-defense in response to any unlawful *armed* use of force.<sup>417</sup>

Most probable is what I would call “cake and eat it too” drafting—everybody gets what they want. Nations wanting to ensure the Charter would not prohibit self-defense (the U.S.) can point to “nothing . . . shall impair,”<sup>418</sup> while those nations with recent, valid fears of powerful neighbors could point to the “if an armed attack occurs.”<sup>419</sup> While, none of the drafters were naïve enough to believe that a post-Charter era would be a war-free utopia, especially with the origins of the Cold War already clearly forming, few would have believed that the Security Council system would be as ineffective as history has proved.<sup>420</sup>

---

411. See Brian Hunt, *Plain Language in Legislative Drafting: An Achievable Objective or a Laudable Ideal?*, 24 STATUTE L. REV. 112, 113 (2003) (attempting to identify the role and purpose of the language used for legislative drafting).

412. But see Michael Akehurst, *Humanitarian Intervention*, in INTERVENTION IN WORLD POLITICS 95, 116 (Hedley Bull ed., 1984) (arguing that the legislative intent of U.N. Charter Art. 2(4) was to strengthen the prohibition on the use of force).

413. See U.N. Charter art. 2, ¶ 4 (laying out the different terms “armed attack” from “use of force”).

414. See U.N. Charter art. 51 (asserting member states’ right to use self-defense).

415. *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 195 (June 27).

416. See *id.* (clarifying the lower standard implied by “armed attack” than “aggression”).

417. Compare U.N. Charter art. 2, ¶, with *Military and Paramilitary Activities*, 1986 I.C.J., ¶¶ 232–33, 235, 238, 249 (addressing the Court’s view of the proper mechanisms for collective self-defense and response to use of force).

418. See U.N. Charter art. 51.

419. *Id.*

420. See Franck, *supra* note 10, at 809 (demonstrating how the five permanent

An alternate explanation is that the “if an armed attack occurs”<sup>421</sup> language was not intended to differentiate the gravity between “armed attack”<sup>422</sup> and “use of force,”<sup>423</sup> but to limit self-defense to be used only *after* a use of force occurred.<sup>424</sup> This argument, however, would be at odds with many of the No Gap School’s adherents other thinking on preemptive self-defense.<sup>425</sup> Putting aside a discussion of preemptive uses of force, there is reasonableness to the interpretation that the wording “if an armed attack occurs”<sup>426</sup> does not modify the scale threshold, only the temporality of *when* self-defense is authorized.<sup>427</sup>

Unlike the overly complicated, subjectivity of the Scale and Effects test, the simplicity of the No Gap School’s analysis transfers effortlessly to the cyber domain.<sup>428</sup> Any unlawful use of force authorizes counterforce in self-defense.<sup>429</sup> Where the Tallinn Manual struggled, the No Gap School would require very little effort to define any of our three cyberwarfare examples as justifying self-defense: 1) Stuxnet, 2) an attack causing a stock market crash, and 3) the 2007 Estonia attacks.<sup>430</sup> Conceptually, any unlawful use of force, even destroying one bit of data, justifies the use of self-defense. However, it seems obvious that no one, now or at the drafting of the Charter, wants states to begin full-scale wars over truly minor incidents.<sup>431</sup> The No Gap School sees the principle of proportionality being the buffer to this concern, “the gravity of an attack may affect the proper scope

---

Security Council members have eroded the protections of Art. 2(4)).

421. See U.N. Charter art. 51.

422. *Id.*

423. See U.N. Charter art. 2, ¶ 4.

424. See U.N. Charter art. 51.

425. See William H. Taft IV, *Preemptive Action in Self-Defense*, 98 PROC. AM. SOC. INT’L L. ANN. MEETING 331, 331–32 (2004) (identifying the contexts in which preemptive self-defense is an acceptable response).

426. See U.N. Charter art. 51 [hereinafter Taft, *Preemptive Action*].

427. See Taft, *Preemptive Action*, *supra* note 426, at 332–33 (further clarifying when U.S. law permits preemptive self-defense).

428. See TALLINN MANUAL 2.0, *supra* note 4, at 126, 333.

429. See Taft *Preemptive Action*, *supra* note 426, at 332–33 (further arguing when U.S. law permits preemptive self-defense).

430. Compare TALLINN MANUAL 2.0, *supra* note 4, at 138–39, 341–42 (admitting that the law is unclear on which types of cyber activity might qualify as an armed attack), with McGuinness, *supra* note 30.

431. See Sofaer, *supra* note 346, at 427–28 (raising the possibility that the No Gap school would reduce the effectiveness of existing interpretations of the Charter).

of the defensive use of force . . . , but it is not relevant to determining whether there is a right of self-defense in the first instance.”<sup>432</sup> Further, policy and politics will also be a check against full scale wars—accountability imbued in the classic distinction between “can” and “should.”

Predictively, this School is certainly closer to the way states behave. As with countermeasures, self-defense cannot be used as retaliation,<sup>433</sup> so there must be an ongoing use of force.<sup>434</sup> Still, as with the U.S. attacks in Libya after the German nightclub bombing,<sup>435</sup> states will *still* employ “creative fictions”<sup>436</sup> to justify self-defense.<sup>437</sup> These creative fictions, however, are relative to the *necessity* rather than the scale and are just as likely as in the scale and effects test.<sup>438</sup>

Descriptively, the No Gaps School downplays arguments over the obvious textual disconnect between Articles 2(4) and 51.<sup>439</sup> The School’s wholesale dismissal of the *Nicaragua* judgment is correct. First, as previously discussed, the *Nicaragua* decision is, at best, a judicial foul ball, an absolute miss in terms of what the law is and how to apply it.<sup>440</sup> Secondly, ICJ opinions are only binding on the parties concerned and only in the current dispute.<sup>441</sup> Whatever precedential value ICJ decisions have, they are only as “a subsidiary means for determination of the rule of law,” valued at the same level of importance as “the teachings of the most highly qualified publicists.”<sup>442</sup> Customary law is a primary source, considered superior

---

432. See Taft, *Self-Defense*, *supra* note 174, at 300 (questioning whether there is a gravity requirement to justify collective self-defense).

433. See DINSTEIN *supra* note 339, at 184 (identifying the difficulty in defining proportionality).

434. See Taft, *Self-Defense*, *supra* note 174, at 302–06 (addressing the United States’ position of accepting the principle of distinction in self-defense).

435. See McCredie, *supra* note 371, at 216.

436. See FRANCK, *supra* note 292, at 112 (acknowledging that states use convenient legal fictions to justify uses of force).

437. See *id.* (providing examples of the legal fictions used to justify uses of force).

438. *Id.*

439. See Sofaer, *supra* note 346, at 422–28 (objecting to the No Gap school as tolerating a restrictive interpretation of Article 2(4)).

440. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶¶ 191, 195 (June 27).

441. See Netherlands Letter, *supra* note 101.

442. ICJ Statute, *supra* note 144, art. 38 ¶ 1(d).

to judicial decisions, and discerned by “international custom, as evidence of a general practice of accepted law.”<sup>443</sup> Further, from the Vienna Convention of the Law of Treaties, “any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation.”<sup>444</sup> States, as evidenced by the preceding discussion,<sup>445</sup> may not be in general agreement; however, there *certainly* is a frequent practice of using self-defense in response to any unlawful use of force.<sup>446</sup> While the Scale and Effects School (and to a lesser degree, the Forceful Countermeasures School) attempts to adhere to a textual and judicial interpretation of the Charter, they essentially disregard state practice and state speech entirely.<sup>447</sup> While there are certainly challenges with all of the Schools’ readings of the text, state practice is much more straightforward.<sup>448</sup> One need not go all the way over to the Charter-is-Dead thinking to still preserve a logical interpretation of the text that mostly conforms to practice, or, at least, what states say when justifying force.<sup>449</sup> As a descriptive matter, the No Gap School expresses an intellectually constant interpretation of the Charter text, accommodating for subsequent state practice.<sup>450</sup> Further, the interpretation is not only workable, but also much less of a victim to subjectivity than the scale and effects test.<sup>451</sup>

---

443. *Id.* art. 38 ¶ 1(b).

444. Vienna Convention on the Law of Treaties, art. 31 ¶ 3(b), 1155 U.N.T.S. 331 [hereinafter Vienna Convention].

445. *See* Taft, *Self-Defense*, *supra* note 174, at 303 (recognizing international consensus that states use self-defense when attacked).

446. *See id.* (recognizing international consensus that states use self-defense when attacked).

447. *See* JAMES A. GREEN, *THE INTERNATIONAL COURT OF JUSTICE AND SELF-DEFENCE IN INTERNATIONAL LAW* 128, 132 (2009) (differentiating between state speech and state action).

448. *But see* Franck, *supra* note 10, at 809 (arguing that the lack of clarity in the Charter allows state practice to erode the Charter).

449. *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶¶ 74, 248, 252, 282 (June 27) (Addressing the fact that states may invoke self-defense to take actions that would otherwise be wrongful).

450. *See* Sofaer, *supra* note 346, at 425 (rejecting the ICJ’s differentiation between “armed attack” and “countermeasures”).

451. *See* Taft, *Self-Defense*, *supra* note 174, at 300–01 (referencing the “gravity” test as subjective).



Prescriptively, the No Gap School also provides the most desirable outcome.<sup>452</sup> First, as with all but the Charter-is-Dead School, force is clearly unlawful, but once used, self-defense becomes lawful.<sup>453</sup> The No Gap framing entirely does away with the messy, unworkable forceful countermeasures system, while still giving states a credible and useable means to challenge original unlawful uses of force.<sup>454</sup> Contrary to the perceived bias of the Court in *Nicaragua*,<sup>455</sup> this framing would lead to less violence, not more, by creating a bright line rule not subject to the subjectivity of the scale and effects test,<sup>456</sup> which otherwise “would encourage states to engage in a series of small-scale military attacks, in the hopes that they could do so without being subject to defensive responses.”<sup>457</sup> While powerful states will always use force in their best interest, a bright line rule will simply separate unlawful from lawful force.<sup>458</sup>

The most credible counterargument to the No Gap lens is that any unlawful use of force, potentially even the destruction of one bit of data, could lead to full-scale war.<sup>459</sup> As discussed, this fear is unfounded legally because of both adherence to the principle of proportionality and the long-held belief that self-defense would only be appropriate in response to an unlawful use of force.<sup>460</sup>

One could also argue that No Gap would simply be substituting one

---

452. See *id.* at 298–99 (expressing that the U.S. does not believe that the ICJ intended to impose such harsh limitations in the *Oil Platforms* decision).

453. *Id.* at 302–03 (explaining proportionality).

454. *Id.* at 302–05 (addressing the right to self-defense and further explaining proportionality).

455. See Paul Lewis, *World Court Supports Nicaragua After U.S. Rejected Judges' Role*, N.Y. TIMES (June 28, 1986), <https://www.nytimes.com/1986/06/28/world/world-court-supports-nicaragua-after-us-rejected-judges-role.html> (identifying earlier tensions between the U.S. and the ICJ).

456. See Taft, *Self-Defense*, *supra* note 174, at 300–01 (expressing skepticism over an objective gravity standard).

457. *Id.* at 300–01. (“Moreover, if States were required to wait until attacks reached a high level before responding with force, their eventual response, would likely be much greater, making it more difficult to prevent disputes from escalating to full-scale military conflicts.”).

458. See Lewis, *supra* note 455.

459. Taft, *Self-Defense*, *supra* note 174, at 300–01.

460. See *id.* at 302–05 (Addressing states' right to self-defense).

subjective standard, “scale and effects,” for another, “proportionality.”<sup>461</sup> However, proportionality is a preexisting concept in international law, with a much stronger consensus than the scale and effects test in customary, judicial, and academic debate.<sup>462</sup> Secondly, proportionality would still exist within self-defense of the Scale and Effects School,<sup>463</sup> so the No Gap School would not be substituting one subjectivity for another, but simply subtracting one of the subjective elements.<sup>464</sup> Admittedly, the importance of proportionality would obviously be higher, moving away from a “scale and effects” gravity threshold.<sup>465</sup>

In determining what unlawful force in the cyber domain looks like, it is helpful to recall our three comparisons: electronic jamming versus destroying communication networks; economic sanctions versus blockades; and espionage versus sabotage.<sup>466</sup> Again, as previously discussed,<sup>467</sup> jamming is perhaps illegal, but not generally viewed as a use of force, whereas the destruction of communication networks would be.<sup>468</sup> Therefore, self-defense would not be lawful in response

461. Katherine Vorderbruggen, *A Rules-Based System? Compliance and Obligation in International Law*, E-INT’L REL. (Oct. 9, 2018), <https://www.e-ir.info/2018/10/09/a-rules-based-system-compliance-and-obligation-in-international-law/> (noting that powerful states will always act in their own self-interest).

462. See Taft, *Self-Defense*, *supra* note 174, at 305 (further addressing proportionality); TALLINN MANUAL 2.0, *supra* note 4, at 127–30, 348–50 (distinguishing countermeasure proportionality from the law of attack proportionality); FRANCK, *supra* note 292, at 91 (questioning the proportionality of large-scale self-defense responses to actions by terrorist bases of operation); DINSTEIN, *supra* note 339, at 185–86 (identifying a two-step process in which a state decides to use self-defense and an international forum gauges the legality of the response).

463. *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 194 (June 27) (identifying necessity and proportionality as the prerequisites to self-defense actions).

464. Compare U.N. Charter art. 51, with *Nicaragua*, 1986 I.C.J., ¶ 194 (examining scale and effects against proportionality). See also Taft, *Self-Defense*, *supra* note 174, at 299–300.

465. See Dinstein, *supra* note 32, at 109 (supporting a single large response to several smaller initial aggressions).

466. See TALLINN MANUAL 2.0, *supra* note 4, at 141–42 (defining cyber warfare).

467. See United Nations Convention of the Law of the Sea art. 109, Dec. 10, 1982, 1833 U.N.T.S. 397.

468. Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817,

to a cyber-attack that resembled short-term jamming, while it would be lawful when an attack more fully resembles the destruction or even partial destruction of communication networks, which would be considered both unlawful and a use of force.<sup>469</sup>

Likewise, with economic sanctions versus a blockade, while both fundamentally target the economic capacity of another state, there is a fundamental difference between sanctions, tariffs, or trade practice and a blockade, the former being both lawful (absent a treaty obligation) and non-forceful, the latter being both unlawful and forceful.<sup>470</sup> The view that economic pressures cannot be uses of force is understandable and desirable, but there is a fundamental difference between national policies that have detrimental economic effects in another nation and acts that enter the sovereign space of another state (even digitally) and prevent its access to global markets.<sup>471</sup>

The Tallinn Manual does excellent work in the area of advancing ideas of sovereignty in the cyber sphere;<sup>472</sup> however, there is still much-needed development in the outline of cyber sovereignty.<sup>473</sup> The manner in which data moves--potentially through all states, as well as international spaces—there are many overlaps between the early days

---

821 (2012) (defining “cyber-attack”).

469. *Id.*; TALLINN MANUAL 2.0, *supra* note 4, at 141–42.

470. See Daniel McCormack & Henry Pascoe, *Sanctions and Preventive War*, 61 J. CONFLICT RESOL. 1711, 1715 (2017) (discussing how sanctions affect relative power).

471. See *id.* at 1729 (“When sanctions bind too tightly, they may cause, rather than help avoid, conflict. In fact, the global shock to oil prices that helped to collapse the ruble in late 2014 may augur for a weakening of sanctions.”).

472. See generally TALLINN MANUAL 2.0, *supra* note 4, at 11–29 (outlining the different iterations of state sovereignty and their applications in cyberspace). But see *id.* at 12 (rejecting an application of various zones to differing levels of sovereignty, stating, “It also is sometimes suggested that it should be assimilated to the high seas, international airspace, or outer space in the sense that of constituting a ‘global common’ . . . While such characterizations may be useful in other than legal contexts, the International Group of Experts did not adopt them on the ground that they disregard the territorial features of cyberspace.”).

473. See *id.* at 3 (“[B]ecause State cyber practice is mostly classified and publicly available expressions of *opinio juris* are sparse, it is difficult to definitively identify any cyber- specific customary international law.”); ASHLEY S. BOYLE, MOVING TOWARD TALLINN: DRAFTING THE SHAPE OF CYBER WARFARE 1 (2012) (noting that “high-profile cyber operations have underscored the need for explicit codes of conduct in international cyberspace”).

of the law of the sea and the cyber world.<sup>474</sup>

Today, we are likely in a cyber-version of Grotius' *Mare Librium* or free seas.<sup>475</sup> Then, like now, there is (mostly) room for everyone.<sup>476</sup> The harvest of the cyber oceans are abundant and enough for everyone.<sup>477</sup> A state still cannot control beyond what a cannon can hit from their shores.<sup>478</sup> But, far quicker than from the time of Grotius to the UN Convention on the Law of Seas, there may emerge some greater ability to control cyber space or detrimental actions that infringe on the sovereignty of others.<sup>479</sup> Even if an ability to control cyberspace does not develop, the desire to better clarify domains will.<sup>480</sup> While not the focus of this writing, I encourage future legal development in this area of separating spaces, with differing degrees of sovereignty, expectations, and rights in different zones. Not perfectly congruent, the zones established in UNCLOS, internal waters, territorial seas, and exclusive economic zones and high seas, as well as the concept of innocent passage have salience in our understanding of cyberspace sovereignty.<sup>481</sup>

---

474. See Peter Dombrowski & Chris C. Demchak, *Cyber War, Cybered Conflict, and the Maritime Domain*, 67 NAVAL WAR COLL. REV. 71, 72–73 (2014) (introducing the challenges and opportunities of cyberspace for U.S. national security).

475. HUGO GROTIUS, *MARE LIBERUM* (David Armitage, ed. 2004); see generally TALLINN MANUAL 2.0, *supra* note 4, at 11–29 (discussing the principle of sovereignty within the cyberspace).

476. See TALLINN MANUAL 2.0, *supra* note 4, at 12 (describing cyberspace as a “global domain”).

477. *Id.*

478. See H. S. K. Kent, *The Historical Origins of the Three-Mile Limit*, 48 AM. J. INT'L L. 537, 537–38 (1954) (discussing the cannon-shot rule).

479. See Max Smeets, *The Strategic Promise of Offensive Cyber Operations*, 12 STRATEGIC STUD. Q. 90, 90–91 (2018) (discussing theoretical parameters of effective military operations).

480. See generally TALLINN MANUAL 2.0, *supra* note 4, at 12, 232–99 (discussing sovereignty, law of the sea, air law, space law, and international telecommunications law).

481. See William M. Stahl, *The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity*, 40 GA. J. INT'L & COMPAR. L. 247, 251 (2011) (noting that UNCLOS “addresses the duty of sovereign states to combat piracy outside its jurisdiction, including in international waters”); United Nations Convention of the Law of the Sea, *supra* note 271, pmb.; JACK GOLDSMITH & TIM WU, *WHO CONTROLS THE INTERNET? ILLUSIONS IN A BORDERLESS WORLD* 1–10 (2006) (discussing territorial questions

The power of the cyber domain is that it is not a physical space in the most conventional sense, yet it works like a bridge, connecting people, while also creating news spaces, traversed by all.<sup>482</sup> When a European sends an email to Singapore, it does not pass through all the territories across Europe and Asia, eventually passing into Thailand, then Malaysia, finally stopping at its destination.<sup>483</sup> Neither does it hop on the ‘high seas’ of the internet and ‘sail’ extra-territorially through the Mediterranean, through the Suez, to the India Ocean, Straits of Malacca, arriving in the port of Singapore.<sup>484</sup> It gets broken into the millions of bits of data and travels everywhere at once finding the path of least resistance<sup>485</sup>—the parallels to water are unmistakable.<sup>486</sup> This “liquidity” poses interesting questions about how one state would send a cyber weapon into another: is it not simply crossing that final international border that poses a potential international trespass, but also every state in between.<sup>487</sup> Is there a concept of innocent passage? What about malware that has the potential to infect everywhere, but is only specifically activated in a selected target later? These questions are unanswerable now, but once better consensus can be achieved,

---

related to cyberspace).

482. See Glenn Alexander Crowther, *The Cyber Domain*, 2 CYBER DEF. REV. 63, 63 (2017) (mentioning that cyberspace is defined as a global domain in the information environment).

483. See Steven Li, *How Does the Internet Work?*, MEDIUM (Aug. 1, 2017), <https://medium.com/@User3141592/how-does-the-internet-work-edc2e22e7eb8> (discussing how packet routing networks move data from their source to their destination).

484. *Id.*

485. *Id.*

486. See U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE CYBERSPACE POLICY REPORT: A REPORT TO CONGRESS PURSUANT TO THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011, SECTION 934 8 (2011) (“The issue of the legality of transporting cyber ‘weapons’ across the Internet through the infrastructure owned and/or located in neutral third countries without obtaining the equivalent of ‘overflight rights.’ . . . The interconnected nature of cyberspace poses significant challenges for applying some of the legal frameworks developed for specific physical domains. The law of armed conflict and customary international law, however, provide a strong basis to apply such norms to cyberspace governing responsible state behavior. Significant multinational work remains to clarify the application of norms and principles of customary international law to cyberspace.”).

487. See *id.* (“The interconnected nature of cyberspace poses significant challenges for applying some of the legal frameworks developed for specific physical domains.”).

both the dialogue and conclusions reached will inform the ultimate question of lawfulness of cyber operations. For now, when considering the unlawfulness of cyber operations, we are confined to a *Mare Librium* context—a cyberspace without much developed law or control.<sup>488</sup>

Finally, the comparison of espionage versus sabotage. Espionage, likely lawful (internationally), is not a use of force, and therefore self-defense is not justified.<sup>489</sup> Sabotage is, again, both unlawful and a use of force.<sup>490</sup> Therefore, a purely cyber spying operation, would not authorize self-defense, whereas a cyber-sabotage operation, like Stuxnet, with or without physical effects, would.<sup>491</sup>

An interesting consideration is a cyber-spying operation that causes some damage on the path to the desired data. While I have advanced what can only be seen as a hardline view that *any* digital damage could constitute a use of force justifying self-defense,<sup>492</sup> *some* reasonableness should apply. The intent of the cyber spy should not be considered relevant, however, as with what might be called “traditional espionage,” there may be a “forceful entry” to the space containing the information sought, such as a broken lock or door, that would not rise

---

488. GROTIUS, *supra* note 475; *See generally* TALLINN MANUAL 2.0, *supra* note 4, at 11–29 (discussing the principle of sovereignty within the cyberspace).

489. *See* Beth D. Grabowitz et al., *Why the Law of Armed Conflict (LOAC) Must Be Expanded to Cover Vital Civilian Data*, 5 CYBER DEF. REV. 121, 125–26 (2020) (stating that manipulating or targeting data during cyber espionage is unprotected under the Law of Armed Conflict).

490. *See* Silver, *supra* note 3, at 73, 75 (asserting that computer network attacks are likely considered force under Article 2(4) of the UN Charter).

491. *See* Grabowitz et al., *supra* note 489, at 125–26 (citing experts whose majority opinion in the Tallum Manual was that a cyber-attack on a State’s infrastructure violated sovereignty if it created damage); Silver, *supra* note 3, at 75 (“[C]ertain applications of CNA are likely to be held to constitute force under Article 2(4), but many applications are likely not to.”); Irving Lachow, *The Stuxnet Enigma: Implications for the Future of Cybersecurity*, 11 GEO. J. INT’L AFFS. (SPECIAL ISSUE) 118, 125 (2011) (“These response options must encompass measures to minimize the damage caused by a Stuxnet-like attack, to enable rapid reconstitution of necessary capabilities, and to take actions (if desired) against the perpetrators of such an attack.”).

492. *See* Silver, *supra* note 3, at 75 (noting that a school of thought, focusing on the malicious and destructive nature of computer network attacks, advocates that the attacks should be considered a prohibited use of force under Article 2(4) of the UN Charter).

to the level of sabotage.<sup>493</sup> There should be some similar exception to what could be called the “broken lock rule” in the cyber domain.<sup>494</sup> Espionage is certainly unlawful in domestic systems, and perpetrators expose themselves to criminal domestic prosecution.<sup>495</sup> Breaking a code or other digital protection—i.e. *truly* minor damage—while stealing information should not be viewed as a use of force. There must be some floor to a use of force.

Finally, regarding prescriptive analysis of what the law should be, as previously discussed,<sup>496</sup> fears that the No Gap School will lead to full-scale war are unfounded because principles of necessity and proportionality will be substantial checks on self-defense in response.<sup>497</sup> Firstly, “there is no legal requirement that the response in self-defense to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality.”<sup>498</sup> While physical force certainly can be used in response to unlawful cyber force, necessity and proportionality would govern that the force used is *necessary* to stop the attack.<sup>499</sup> This lower bar to the threshold of self-defense certainly seems desirable for power states in conventional domains,<sup>500</sup> but Ryan Goodman posits, that because the U.S. has the most to defend, militarily, economically, etc. the deterrence effect of dominate conventional force may not be as effective as in the cyber domain, where attribution will be quite difficult.<sup>501</sup> Moreover, for the force to be necessary, the attack must be ongoing or at least reasonably believed to not have stopped.<sup>502</sup> Any

---

493. See *id.* at 76–77 (listing several purposes for cyber intrusions).

494. See *id.* at 75.

495. Espionage Act, 22 U.S.C. § 406 (2014).

496. Dinstein, *supra* note 32, at 109; TALLINN MANUAL 2.0, *supra* note 4, at 11–29.

497. See Schmitt II, *supra* note 252, at 913 (arguing that proportionality balances positive consequences against harmful ones).

498. DoD LAW OF WAR MANUAL, *supra* note 403, at 1017.

499. Hathaway et al., *supra* note 468, at 849 (noting that evaluating whether self-defense complies with necessity and proportionality is increasingly difficult with cyber-attacks).

500. *Id.* at 850 (discussing *ad bellum* and *in bello* necessity and proportionality).

501. Ryan Goodman, *Cyber Operations and the U.S. Definition of “Armed Attack”*, JUST SEC. (Mar. 8, 2018), <https://www.justsecurity.org/53495/cyber-operations-u-s-definition-armed-attack>.

502. See *id.* (“[I]n a world in which States very frequently engage in low-level

force used after a completed and final attack is simply retaliation, not self-defense.<sup>503</sup>

The pin-prick scenario is again helpful here: assuming the likelihood of an ongoing series of small attacks, the No Gap School would be unconcerned whether the collection aggregated to an armed attack.<sup>504</sup> The first prick, in and of itself, would constitute an unlawful use of force surpassing the threshold question justifying self-defense.<sup>505</sup> Thereafter, the ongoing series of attacks creates the necessity to use force in response.<sup>506</sup> Proportionality is not viewed in relation to the scale of the original attack, but in relation to the necessity to stop the attack.<sup>507</sup> Full-scale war will never be the lawful response to an attack that can be reasonably stopped with a hack-back or even a single missile-strike.<sup>508</sup>

Necessity and proportionality are certainly not principles that are exclusive to the No Gap School, but they are the guard rails the Court in *Nicaragua* failed to use effectively.<sup>509</sup> Because of the lower

---

uses of force in cyber, or might be thought to have done so by their adversaries . . . many States will have the legal right to use force in self-defense against others on an ongoing basis.”).

503. See Dinstein, *supra* note 32, at 184–85 (expressing that this idea is embodied within the principles of necessity and immediacy but that this “condition must be construed ‘broadly.’ . . . [a] lapse of time is almost unavoidable.”).

504. See GRAY, *supra* note 132, at 107 (“In cases of repeated cross-border incursions commentators have spoken of the ‘accumulation of events’ or ‘pin-prick’ theory of armed attack in order to justify otherwise disproportionate response. That is, they claim that states may use force not in response to each incursion in isolation but to the whole series of incursions as collectively amounting to an armed attack.”).

505. *Id.*

506. *Id.*

507. See Hargrove, *supra* note 49, at 136 (“The essence of the Charter principles is that . . . a state must refrain from using force against other states, except where force is being used against it. In that case, it is free to defend itself with force as best it can, provided only that its response is reasonably proportionate to the injury being inflicted and, in fact, necessary to put an end to it.”); see also Taft, *Self-Defense*, *supra* note 174, at 305 (“There is no requirement in international law that a State exercising its right of self-defense must use the same degree or type of force used by the attacking State in its most recent attack. Rather, the proportionality of the measures taken in self-defense is to be judged according to the nature of the threat being addressed.”).

508. See Hargrove, *supra* note 49 (“[R]esponse [to an attack must be] reasonably proportionate to the injury being inflicted.”).

509. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v.



threshold of the No Gap School for the use of self-defense, these principles become all the more important.<sup>510</sup> Necessity and proportionality become a better and more reasonable means of regulating state behavior than the scale and effects test.<sup>511</sup> When compared from a factual perspective, state responses to force might appear similar to the Forceful Countermeasures School--small scale attacks producing small scale responses.<sup>512</sup> But the use of the No Gap legal framing does not produce the messy "quadruple structure"<sup>513</sup> analysis Dinstein attributed to the Court in *Nicaragua* force short of an armed attack, responded to with force short of self-defense, with the aggressor state then justifying self-defense in response to an excessively forceful countermeasure.<sup>514</sup> The legal analysis effectively stops, as in the schoolyard with: "who started it."<sup>515</sup>

## XI. CONCLUSION

Each of these schools have intellectual and practical advantages and drawbacks, especially when considering cyber operations.<sup>516</sup> Either they depart from the language of the Charter, moderately to substantially (Scale and Effects, No Gap, Counter-Measures, Charter-

---

U.S.), Judgment, 1986 I.C.J. 14, ¶ 237 (June 27).

510. See Schmitt, *supra* note 204, at 913 (discussing the value of the principle of proportionality).

511. See Hathaway et al., *supra* note 468, at 850 (discussing *in bello* necessity and proportionality); Dinstein, *supra* note 32, at 109 (discussing the three conditions of self-defense: necessity, proportionality, and immediacy); Hargrove, *supra* note 49, at 136 (asserting that under the Charter principles, States must not use force unless another State is using force against it); Taft, *Self-Defense*, *supra* note 174, at 305 (asserting that international law does not require proportionality).

512. See Dinstein, *supra* note 32, at 109 ("The counter-measures taken by State B (kinetically or electronically) must not be out of proportion with the act prompting them. A modicum of symmetry between force and counter-force—injury inflicted on State B by the armed attack versus damage sustained by State A by dint of self-defense counter-measures—is called for.").

513. DINSTEIN, *supra* note 339.

514. *Military and Paramilitary Activities*, 1986 I.C.J., ¶ 237.

515. See *id.* (finding that "the reaction of the United States in the context of what it regarded as self-defence was continued long after the period in which any presumed armed attack by Nicaragua could reasonably be contemplated.").

516. Hathaway et al., *supra* note 468, at 851 (discussing the unique challenges of the proportionality and analysis of cyber-attacks).

Is-Dead),<sup>517</sup> and/or they come to potentially undesired results (Scale and Effects--no right to respond to force short of an armed attack;<sup>518</sup> Forceful Countermeasures—limited right to respond;<sup>519</sup> and Charter-Is-Dead—no rules whatsoever).<sup>520</sup> There is strong intellectual honesty in dealing with state practice in both the Charter-Is-Dead and a weak-hearted Charter-Is-Dead justification for Forceful Countermeasures.<sup>521</sup> Both identify the source of the problem (state abuse) and that the UN systems do not work in the manner conceived, but their solutions are unwieldy.<sup>522</sup> With the strong possibility and severity of future cyber warfare, only the dominant Scale and Effects School fails entirely to provide a clear remedy to such flagrant uses of force such as Stuxnet, an attack causing a stock market crash, or the 2007 Estonia attack.

The Charter-Is-Dead School certainly has a strong predictive view on how states will behave, particularly powerful states, particularly in the cyber domain.<sup>523</sup> The Charter-is-Dead would argue descriptively that there is no rule preventing cyber-attacks because there is no longer (or never really was) law preventing the use of force due to widespread state disregard.<sup>524</sup>

The No Gap School, however, is closer to how states will behave *and* importantly, what they will say when they use force.<sup>525</sup> When attacked with cyber means, especially where there are no physical

---

517. Hathaway et al., *supra* note 468, at 850; Dinstein, *supra* note 32, at 110; Hargrove, *supra* note 49, at 136; Taft, *Self-Defense*, *supra* note 174, at 305.

518. Hathaway et al., *supra* note 468, at 850 (“A state’s use of armed force in response to a cyber-attack must not only conform with U.N. Charter and customary international law limits on the use of armed force, but it must also comply with the *jus ad bellum* principles of necessity and proportionality under customary international law.”).

519. See Dinstein, *supra* note 32, at 109.

520. See Murphy, *supra* note 11, at 717–18 (explaining the school of thought that believe the Charter’s rules on the use of force are “completely devoid of any legal significant normative value.”).

521. See *id.* at 715–18 (comparing the Qualitative Threat school and the Charter-Is-Dead school).

522. *Id.*

523. See Murphy, *supra* note 11, at 717–18 (outlining the views of the Charter-Is-Dead school).

524. *Id.*

525. See generally Abraham D. Sofaer, *International Law and the Use of Force*, 13 NAT’L INT. 53, 54–59 (1988) (providing a historical overview on the United States’ position on the No Gap School and decisions regarding use of force).

effects, as in situations like the 2007 Estonia attacks and the stock market crash scenarios, if a state has the means to stop the attack with physical or cyber means, and it is in their interests, they will.<sup>526</sup> Most likely, states will argue such a cyber-attack is an “armed attack” (regardless of the test applied) and will respond in self-defense.<sup>527</sup> Only the No Gap School would accurately describe this justification as a lawful response in self-defense to an unlawful use of force.

It would be overly ambitious to attempt to resolve fundamental, long-debated disagreements about how to read the language of Articles 2(4) and 51.<sup>528</sup> However, analysis applied by the majority Scale and Effects School, especially when thinking about cyber force, is unrealistic, unworkable, and undesirable for state actors.<sup>529</sup> If proportionality still governs all uses of counterforce (countermeasures or self-defense) in response to cyber force, then it is tempting to assign the entirety of the forgoing argument to the merely academic realm.<sup>530</sup> But, especially considering the varying domestic legal prohibitions against violations of international law of many of the United States’ closest allies, getting the law right is vitally important.<sup>531</sup> The domestic

---

526. *Id.*; see Taft, *Self-Defense*, *supra* note 174, at 305 (quoting Judge Roberto Ago, who explained, “What matters [with respect to proportionality] is the result to be achieved by the ‘defensive’ action, and not the forms, substance and strength of the action itself.”).

527. See Hargrove, *supra* note 49, at 136 (“[U]nless the use of force has been internationally authorized, a state must refrain from using force against other states, except where force is being used against it.”); see Hathaway et al., *supra* note 468, at 850 (“Although a stand-alone cyber-attack has never instigated an armed conflict, cyber-attacks have been used in wars in response to traditional provocations or to prepare the way for an imminent conventional attack.”).

528. See Silver, *supra* note 3, at 75 (“It is too early for any legal authority to have emerged on the status of CNA under Article 2(4).”); see also Hargrove, *supra* note 49, at 139 (“Any suggestion that there are any acts of unlawful force between states that international law forbids a state from defending against by proportionate force . . . degrades the concept of international law and diminishes the inducement for a responsible political leader to take its constraints seriously.”).

529. Dinstein, *supra* note 32, at 100 (noting that the choice of words in Article 51 is “deliberately restrictive” and leaves little effective protection against states who violate the use of force prohibition).

530. See, e.g., Hathaway et al., *supra* note 468; Dinstein, *supra* note 32; Hargrove, *supra* note 49; Taft, *Self-Defense*, *supra* note 174; Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 237 (June 27).

531. See Sofaer, *supra* note 525, at 54–59 (outlining the United States’ position

legal adherence to international law of many nations, the Netherlands in particular, is laudable, but the application of the *Nicaragua* judgment's scale and effects test, as applied to cyber operations in the Tallinn Manual is simply not the law and should not be used to consider uses of force in response to cyberwarfare.<sup>532</sup>

---

regarding the use of force); Taft, *Self-Defense*, *supra* note 174, at 305 (stating proportionality in use of force is not required under international law).

532. TALLINN MANUAL 2.0, *supra* note 4, at 11–29.