Penn State Journal of Law & International Affairs

Volume 11 | Issue 2

May 2023

The Jus Ad Bellum in Cyberspace: A New Framework

M. Walker Brunner

ISSN: 2168-7951

Penn State
Journal of Law & International Affairs

2023 VOLUME 11 NO. 2

THE JUS AD BELLUM IN CYBERSPACE: A NEW FRAMEWORK

By M. Walker Brunner[*]

TABLE OF CONTENTS

[*] Walker Brunner is pursuing his B.S. in Computer Engineering from the Georgia Institute of Technology and was formerly a cadet at the United States Air Force Academy. The author thanks Lieutenant Colonel Timothy Goines, USAF, and Major Logan Sisson, USAF, for their support.

I. INTRODUCTION

Today's societies have become increasingly dependent on the capabilities and opportunities provided by computer systems, networks, and the Internet.[1] As noted by former U.S. Deputy Secretary of Defense William Lynn, "bits and bytes can be as threatening as bullets and bombs."[2] This dependency has created a world in which vital aspects of a state's infrastructures are vulnerable to paralysis through an effective cyberattack.[3] This results in an increased attractiveness for adversarial states to use cyber weapons as instruments in conflict.[4] Because of cyber weapons' newfound importance as weapons of war, their application must be controlled by international restrictions on the use of force. The United Nations (UN) Charter bans the use of force except in instances of self-defense when an "armed attack" has occurred.[5] But the Charter was developed in 1945, far before the advent of cyber capabilities. As a result, customary state practice and decisions from the International Court of Justice (ICJ) have largely focused on conventional warfare.[6] As cyberspace transitions into a warfighting domain, clarity is needed to determine the conditions under which a state may resort to using force—the jus ad bellum criteria.

Jus ad bellum is part of a broader tradition of ethical thought, known as "just war theory."[7] This theory's origins are credited to

---

[1] *See* GEORG KERSCHISCHNIG, CYBERTHREATS AND INTERNATIONAL LAW 7 (2012).

[2] William J. Lynn III, Deputy Sec'y of Def., Remarks on the Department of Defense Cyber Strategy (July 14, 2011).

[3] *War in the Fifth Domain*, THE ECONOMIST (July 1, 2010), https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain.

[4] *See* Lesley Swanson, *The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict*, 32 LOY. L.A. INT'L & COMPAR. L. REV. 303, 205 (2010).

[5] U.N. Charter art. 2, ¶ 4.

[6] *See* MARK WEISBURD, USE OF FORCE: THE PRACTICE OF STATES SINCE WORLD WAR II 25 (1997).

[7] Apart from *jus ad bellum* there are two other subsets of just war theory: *jus in bello* and *jus post bellum*, or proper conduct in and after war, respectively. *See* BRIAN OREND, THE MORALITY OF WAR 20-21 (2013).

Aristotle.[8] Although advanced by Christian thinkers such as Thomas Aquinas and St. Augustine, and later by scholars such as Grotius, Locke, and Vattel, it is fundamentally a secular idea—a framework for evaluating a war's legitimacy.[9] Following World War II, just war theory, which before the war had largely been relegated under the purview of Catholic historians, came to the forefront of international discourse.[10] Ultimately, the UN Charter was the document most significantly involved in codifying jus ad bellum concepts in international law, creating a legal means for states to go to war.[11] While the UN Charter, ICJ cases interpreting its articles, and other international treaties provide guidelines for evaluating the legality of armed force, they are grounded in a long history of philosophical scholarship.[12] Nevertheless, in the current legal regime, four principles predominate: just cause, necessity, proportionality, and public declaration by a proper authority.[13] While each are vital to a complete jus ad bellum framework, this article will focus specifically on addressing proportionality and just cause, while adopting the conventional interpretation of the necessity and public declaration by proper authority principles.[14]

First, this article outlines the current legal framework for jus ad bellum. Next, this article evaluates existing approaches for cyberspace's ability to adequately address the difficulties presented by cyberwarfare. Initially, this article will explore an effects-based approach. Under this approach, the realized effects of a cyberattack are analogized to a conventional kinetic attack to determine whether

---

8 *Id.* at 10.

9 *Id.* at 10-19.

10 *Id.* at 23.

11 *Id.*

12 *Id.* at 20-21.

13 TOM RUYS, 'ARMED ATTACK' AND ARTICLE 51 OF THE UN CHARTER: EVOLUTIONS IN CUSTOMARY LAW AND PRACTICE 53-54, 91 (2011).

14 Public declaration by a proper authority, while an important aspect of the *jus ad bellum* framework, can be widely applied to all general conflicts and a belabored repetition of the principle will not substantively add to this article. *See generally* OREND, *supra* note 7, at 52-59.

just cause for a defensive response is warranted.[15] Following that will be an alternative approach where intended harm to physical systems is the standard for establishing just cause. Because of the shortcomings of these two approaches, this article proffers a new framework. This new framework will create cyber-specific criteria for both just cause and proportionality, breaking from the conventional practice of only developing guidelines for just cause. This model adopts ideas from both the first approach's method of comparing the effects of a cyberattack to those of a kinetic attack and the second approach's intent-based regime, while creating a requirement for the effects to be intransient. By incorporating two methods for approaching proportionality often considered independently of one another, a more realistic, useful, and flexible way to legally evaluate cyberwarfare takes shape. Unlike its alternatives, the framework proposed in this article avoids the pitfalls of malleability, permissiveness, and antiquated restrictions while adhering to the fundamental intent of the UN Charter, providing recourse to states should international peace and security be threatened or breached.

A. Defining Terminology

While different states and organizations have adopted various meanings for the terms cyberspace, cyberattack, cyberwarfare, cyber weapon, and cyber operation,[16] this article will provide definitions for each to avoid confusion in the proceeding discussion and provide a way for a jus ad bellum criterion to be developed. The purpose of this article is not to argue that a provided definition is necessarily more deserving of appropriation than another.

Cyberspace is defined as "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including

---

[15] MICHAEL SCHMITT, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 340-41 (2017) [hereinafter the Tallinn Manual].

[16] Nick Ebner, *Cyber Space, Cyber Attack and Cyber Weapons*, INST. FOR PEACE RSCH. & SEC. POL'Y AT THE UNIV. HAMBURG 2 (Oct. 2015), https://ifsh.de/file-IFAR/pdf_english/IFAR2-FactSheet7.pdf.

the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[17]

The term "cyberattack" will be used frequently and an established definition is vital. This article defines it as:

> A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's . . . cyber systems, assets, or functions. The intended effects of [a] cyberattack are not necessarily limited to the target's computer systems or data themselves . . . A cyberattack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyberattack may be widely separated temporally and geographically from the delivery.[18]

While discussion has arisen as to whether the definition for a cyberattack should adopt a target-based or instrument-based regime,[19] this definition strikes a middle ground by encompassing both. Furthermore, it does not limit the effects of a cyberattack to only computer systems.[20] The term "cyber weapon" will be used to denote the delivery vehicle through which the cyberattack is executed. Although a cyberattack is meant to describe a single hostile act in

---

[17] *Cyberspace,* U.S. DEP'T OF DEF. DICTIONARY OF MIL. & ASSOCIATED TERMS (2021).

[18] U.S. DEPARTMENT OF DEFENSE CYBERSPACE OPERATIONS LEXICON 5, https://info.publicintelligence.net/DoD-JointCyberTerms.pdf (last visited March 2, 2022). The original definition provided by the US DoD includes the term "critical" to describe "cyber systems, assets, or functions." However, because of the proceeding discussion on the threshold between "use of force" and an "armed attack," the use of "critical" has been excluded to provide increased clarity. Therefore, in this essay cyberattack will encompass all such hostile acts regardless of their severity or targeting of critical infrastructure.

[19] Reese Nguyen, *Navigating* Jus Ad Bellum *in the Age of Cyber Warfare*, 101 CAL. L. REV. 1079, 1085-86 (2013).

[20] This article will consider the activation of a cyberattack to include the introduction to a computer system of a time-delayed or conditional delivery vehicle, such as a logic bomb.

cyberspace, the term "cyberwarfare" is more general and meant to encompass the use of cyberspace to conduct armed conflict broadly.[21]

A "cyber operation" encompasses "a cyberattack employed with the primary purpose of achieving objectives in or through cyberspace."[22] Because of the close relationship between cyberattacks and cyber operations, the two will be used synonymously here.

B. The Attribution Problem

The jus ad bellum tradition relies on the ability to impute a cyberattack to a state or non-state entity. Yet, in the cyber domain, anonymity represents one of the greatest assets available to actors.[23] The difficulties in identifying the party ultimately responsible for a cyberattack are a significant technical complication.[24] With the Internet in particular, the ability to conceal the attacker's identity has been a perennial challenge for states wary of using defensive force against a state who was incorrectly identified as an aggressor. It has been noted that "the [I]nternet is one big masquerade ball. You can hide behind aliases, you can hide behind proxy servers, and you can surreptitiously enslave other computers to do your dirty work."[25] However, identifying one's attackers as a result of a disguised attack is not unique to cyberspace. In *Nicaragua v. United States*, the ICJ held that "the problem is not . . . the legal process of imputing the act to a particular state . . . but the prior process of tracing material proof of

---

[21] Ido Kilovaty, *Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare*, 5 AM. U. NAT'L. SEC. L. BRIEF 92, 99 (2014).

[22] The Tallinn Manual, *supra* note 15.

[23] MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 33 (2014).

[24] *Id.*

[25] JOEL BRENNER, AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE 32 (2011). The "Solar Sunrise" attack in 1998 against the U.S. Department of Defense was carried out by an Israeli teenager and students in California with a computer based in the United Arab Emirates. Scott Shackelford & Richard B Andres, *State Responsibility for Cyber Attacks; Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971, 982 (2011).

the identity of the perpetrator."[26] For instance, in international terrorist attacks, the identification of the aggressor has often been a problem.[27] Yet, in cyberspace, as for terrorist attacks, the fact that attribution poses a challenge should not be a reason to neglect the determination of legal implications in cyberspace. Intelligence gathering, traceback tools such as behavior-based algorithms, and other advancements in cyber technology have allowed victim-states to accurately attribute attacks to their perpetrator, despite their difficulty.[28] For these reasons, the difficulties of attribution should not impede the jus ad bellum criteria's evaluation in the cyber domain.

II. JUST CAUSE

A. Foundations

The 1648 Peace of Westphalia brought about an era where states were horizontally organized with no recognized superior authority.[29] The rights of individual states dominated all others and military action was only justified when in defense of the sovereignty of the state. The UN Charter incorporated these ideas into the corpus of international law. In particular, Article 2(4) created a general prohibition against "the threat or use of force against the territorial integrity or political independence of any State, or in any other matter inconsistent with the purposes of the United Nations."[30] Also, Article 51 created an exception to the use of force proscription by protecting a state's "inherent right of individual or collective self-

---

[26] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 57 (June 27).

[27] *See* NAT'L COMM'N ON TERRORIST ACTS UPON THE U.S., THE 9/11 COMMISSION REPORT 76 (2004).

[28] Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17 J. CONFLICT & SEC. L. 229, 233-36 (2012); Jay Kesan & Carol Hayes, *Mitigative Counterstriking: Self-Defence and Deterrence in Cyberspace*, 25 HARV. J. L. & TECH. 430, 482 (2012); OREND, *supra* note 7, at 178.

[29] DAVID FISHER, MORALITY AND WAR: CAN WAR BE JUST IN THE TWENTY-FIRST CENTURY? 69-70 (2012).

[30] U.N. Charter art. 2, ¶ 4.

defense if an armed attack occurs. . . ."[31] This Article enshrines the right to defend against aggression; it legally codifies the notion of a just cause for war. Articles 2(4) and 51 are both considered customary international law, binding on all states regardless of membership to the UN.[32]

Article 2(4) does not explicitly provide a definition of "use of force" although it is generally accepted, at a minimum, to include conventional interpretations of force, including aerial, naval, and land military operations.[33] However, use of force does not include actions considered to be political or economic coercion.[34] Espionage, boycotts, and space-based remote sensing are also not considered uses of force.[35] It is important to understand when a state can engage in a use of force. First, under Article 51, a state can use force when acting in self-defense.[36] Second, actions that qualify as a use of force assist in the determination of what constitutes an armed attack. Nicaragua described an armed attack as a subset of use of force, with not every use of force qualifying as an armed attack.[37] The ICJ held that an armed attack must have a trans-border element and its "scale and effects" should be evaluated to ensure it is of "sufficient gravity."[38] Aside from these criteria, the court only provided specific examples of what is or is not an armed attack.[39] For instance, the court held that minor "trans-border military incursions into the territory" and the "provision of arms to the opposition in another [s]tate" were insufficient to justify force taken in self-defense.[40] The

---

[31] *Id.* at art. 51.

[32] Gary Brown & Keira Poellet, *The Customary International Law of Cyberspace,* 6 STRATEGIC STUD. Q., 126, 126 (2013).

[33] Nguyen, *supra* note 19, at 1,114.

[34] *See id.*; Documents of the United Nations Conference on International Organization, U.N. Doc. 2, G/7(e)(4), 3 U.N.C.I.O. Docs. 251, 252-53 (May 6, 1945).

[35] Nguyen, *supra* note 19, at 1114.

[36] U.N. Charter art. 51.

[37] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 219 (June 27).

[38] *Id.* at ¶ 195.

[39] The Tallinn Manual, *supra* note 15, at 341.

[40] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, 77, ¶ 230 (June 27).

rationale behind delineating between uses of force and an armed attack aims to preserve international peace "before the interest of individual states in the absolute and immediate protection of their sovereign rights."[41]

Despite scant guidance on determining where the line is drawn between use of force and armed attacks, this does preclude a state from responding in self-defense to cyber operations. As found in the ICJ's Nuclear Weapons Advisory Opinion, Articles 51 and 2(4) apply irrespective to the weapon used.[42] And it is "neither the designation of a device, nor its normal use, which make an object a weapon but the intent with which it is used and its effect."[43] Therefore, cyberattacks qualify under Article 51 as possible weapons allowing for a defensive response. Yet, the apparent ambiguity of the UN Charter and the declination of the ICJ to significantly expound on what constitutes uses of force and armed attacks, means there are only basic criteria for determining when a cyberattack constitutes an armed attack.[44]

A contrary perspective on the delineation between uses of force and an armed attack asserts that the difference is either insignificant or non-existent and was overstated by the ICJ in the Nicaragua case.[45] The United States supports this view, asserting that aggressive force of any severity may warrant self-defense.[46] Proportionality and necessity, rather than just cause, primarily limit the actions of the victim-state.[47]

---

41 DEREK BOWETT, SELF-DEFENSE IN INTERNATIONAL LAW 191 (1958).

42 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 39 (July 8).

43 Karl Zemanek, *Armed Attack*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW ¶ 21 (2013).

44 *See* Nils Melzer, *Cyberwarfare and International Law*, U.N. INST. DISARMAMENT RSCH. 13 (Oct. 5, 2011), https://unidir.org/sites/default/files/publication/pdfs//cyberwarfare-and-international-law-382.pdf.

45 The Tallinn Manual, *supra* note 15, at 332.

46 Abraham Sofaer, *International Law and the Use of Force*, 82 AM. SOC'Y INT'L L. PROC., 420, 422 (1988).

47 *Id.*

Regardless of the process through which it is determined whether an act of aggression rises to the level of an armed attack, the requirements of necessity and proportionality must also be met.[48] The necessity condition was acknowledged by the ICJ first in Nicaragua and later in the *Iran v. United States* judgment (hereinafter "Oil Platforms").[49] Components of necessity include the need for the defensive response to be one of last resort, where other means of redress would be futile.[50] This condition maintains unanimous support in current legal doctrine.[51] Additionally, a targeting condition mandates defensive force to target the source of the armed attack.[52] A requirement for immediacy obligates the defensive force to be exercised during or in anticipation of an armed attack,[53] seeking to distinguish actions of self-defense from unlawful reprisals.[54]

---

[48] *See supra* notes 13-14 and accompanying text.

[49] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J.14, ¶¶ 176, 194 (June 27); Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶¶ 43, 73-74, 76 (Dec. 12).

[50] RUYS, *supra* note 13, at 95.

[51] *E.g.*, YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 209-10 (1988); TARCISIO GAZZINI, THE CHANGING RULES ON THE USE OF FORCE IN INTERNATIONAL LAW 144 (2005); DAVID RODIN, WAR AND SELF-DEFENSE 111 (2002).

[52] RUYS, *supra* note 13, at 108. The targeting requirement is classified as an element of proportionality by some authors. However, in *Oil Platforms*, targeting was formed as a subset of the necessity condition. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶¶ 74-76 (Dec. 12). On the other hand, in *Nicaragua*, targeting of certain objects was classified as disproportionate. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 237 (June 27). For purposes of this article, the *Oil Platforms* case will be looked to because of its explicit assessment of the necessity principle and being the more recent decision.

[53] Because a cyberattack points to a general disposition of the aggressor-state, it is warranted for defensive force to be used after the cyberattack is repelled should there be reason to believe a broader attack is not concluded.

[54] RUYS, *supra* note 13, at 99. The immediacy requirement is sometimes considered a separate condition alongside necessity and proportionality. *E.g.*, AVRA CONSTANTINOU, THE RIGHT OF SELF-DEFENCE UNDER CUSTOMARY INTERNATIONAL LAW AND ARTICLE 51 OF THE UNITED NATIONS CHARTER 159-61 (2000); DINSTEIN, *supra* note 51, at 242; GAZZINI, *supra* note 51, at 143-46.

The proportionality condition, enshrined in Articles 22 and 23 of The Hague Convention IV,[55] acts as a constraint on the scale and effects of defensive force.[56] However, unlike the significant consensus enjoyed by the necessity criterion, proportionality is disputed.[57] Nevertheless, fundamental doctrinal approaches have been developed. The most prominent, known as the "means-end" standard,[58] evaluates proportionality with regard to the "aim of the defensive action."[59] As noted by jurist Roberto Ago, "[w]hat matters in this respect is the result to be achieved by the 'defensive' action, and not the forms, substance and strength of the action itself."[60] This theory that proportionality should be considered with regard to the objective of self-defense has been largely adopted by legal scholars.[61]

A second approach is known as "narrow proportionality." Just war theorist Brian Orend defines narrow proportionality as where a state considering just war weighs the "expected universal

---

[55] Hague Convention (IV) Respecting the Laws and Customs of War on Land arts. 22, 23, Oct. 18, 1907, 36 Stat. 2277.

[56] RUYS, *supra* note 13, at 110.

[57] *Id.* This has occurred for several reasons. First, states have failed to create explicit guidelines for its application despite adhering to the general principle. *See* JUDITH GARDAM, NECESSITY, PROPORTIONALITY AND THE USE OF FORCE BY STATES 20 (2004). Further, proportionality is a factor in both *jus in bello* and *jus ad bellum* traditions. OREND, *supra* note 7, at 125. In *jus in bello,* the principle applies to specific attacks and operations; proportionality in *jus ad bellum* encompasses the defensive response in aggregate. *Id.* Scholars have struggled to contend with the overlapping nature of the two, and *jus in bello* considerations have largely dominated. RUYS, *supra* note 13, at 111. Finally, the principle is contextual in nature, making it difficult to create a framework applicable to varying types of defensive uses of force because a multiplicity of considerations are unique to each situation. CONSTANTINOU, *supra* note 54, at 162; GARDAM, *supra* note 57, at 21-22.

[58] *See* David Kretzmer, *The Inherent Right to Self-Defence and Proportionality in* Jus Ad Bellum, 24 EUR. J. INT'L L. 235, 239 (2013).

[59] RUYS, *supra* note 13, at 112.

[60] Roberto Ago (Special Rapporteur), Addendum to the Eighth Rep. on State Responsibility, [1980] Y.B. of the Int'l L. Comm'n, vol. II, pt. 1, 13, 69, U.N. Doc. A/CN.4/318/Add.5-7.

[61] *E.g.*, GAZZINI, *supra* note 51, at 148; Ronald St. John Macdonald, *The Nicaragua Case: New Answers to Old Questions*, 24 CAN. Y.B. INT'L L. 153 (2016); MYERS MCDOUGAL & FLORENTINO FELICIANO, LAW AND MINIMUM WORLD PUBLIC ORDER: THE LEGAL REGULATION OF INTERNATIONAL COERCION 242 (1961); The Tallinn Manual, *supra* note 15, at 349-50.

benefits of doing so against the expected universal costs. Only if the projected benefits, in terms of securing the just cause, are at least equal to, and preferably greater than, such costs as casualties may the war action proceed."[62] The challenges inherent in this calculation—essentially a cost-benefit analysis—are significant because the question of which elements to consider and how may be impossible to quantify with certainty. This approach's relative lack of adoption in the jus ad bellum tradition stems from this uncertainty.[63] Critics of narrow proportionality assert that the commensurate balancing entailed would deprive the victim-state from "effective protection."[64] Thus, the appeal for the means-end approach as a less restrictive and more functional framework becomes more appealing. While scholarship has largely adopted the means-end approach, there is no evidence in customary practice that states prefer this approach over narrow proportionality.[65]

Despite these foundations, there is a lack of academic interest in furthering jus ad bellum proportionality, regardless of the broad consensus advocating for its application.[66] Moreover, discussions of cyber-specific proportionality have revolved around jus in bello considerations, with limited creation of cyber-specific requirements under jus ad bellum.[67]

---

62 OREND, *supra* note 7, at 62.

63 Kretzmer, *supra* note 58, at 278.

64 RUYS, *supra* note 13, at 58.

65 *Id.*

66 Ian Brownlie, *The Use of Force in Self-Defense*, 37 BRIT. Y.B. INT'L L. 183, 229 (1961); CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 150 (2000).

67 *E.g.*, Eric Boylan, *Applying the Law of Proportionality to Cyber Conflict: Suggestions for Practitioners*, 50 VAND. J. TRANSNAT'L L. 217 (2017); Hensey Fenton III, *Proportionality and its Applicability in the Realm of Cyber-Attacks*, 29 DUKE J. COMPAR. & INT'L L. 335 (2019); Peter Pascucci, *Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution*, 26 MINN. J. INT'L L. 419 (2017); Eric Jensen, *Cyber Attacks: Proportionality and Precautions in Attack*, 89 INT'L L. STUD. 198 (2013).

B. Current Approaches

Building from the foundations of international law, scholarship has sought to create lex ferenda analytical frameworks for determining necessary and proportional uses of force when armed attacks in cyberspace occur. These frameworks have largely focused on policy-oriented and ethical considerations.[68] This article will explore two of these existing approaches.[69] First this article reviews the effects-based model put forth by the North Atlantic Treaty Organization's Tallinn Manual on the International Applicable to Cyber Warfare (Tallinn Manual).[70] Second, will be a model classifying armed attacks as intentional force against cyber-physical systems.[71] A summary of each approach will be presented alongside its merits and drawbacks. Neither model can satisfactorily apply relevant international law to the cyber domain in a way that leads to coherent outcomes; a new framework must be offered.

1. Effects-Based Approach (The Tallinn Manual)

This framework analyzes the consequences of a cyberattack with reference to a kinetic attack. Regardless of the means used, if the effects of the cyberattack are "analogous to those that would result from an action otherwise qualifying as a kinetic armed attack," a forceful response to the cyberattack may be warranted.[72] Using the scale and effects criteria from Nicaragua, the authors of the Tallinn Manual agreed that although there is no bright line, some cases of use of force which "injures or kills persons or damages or destroys property would satisfy the scale and effects requirement."[73] Contrarily, acts of cyber espionage, theft, and "brief or periodic interruption of non-essential cyber services" do not warrant a defensive response.[74] The authors remained unresolved as to whether

---

68 Kilovaty, *supra* note 21, at 91-124.

69 Other models include instrument-based and target-based approaches. The inapplicability of these has been addressed and, accordingly, will not be done so in this article. *See* Nguyen, *supra* note 19, at 1117-21.

70 *See generally* The Tallinn Manual, *supra* note 15.

71 Nguyen, *supra* note 19.

72 *Id.* at 340-41.

73 *Id.* at 341.

74 *Id.*

consequences not resulting in death, injury, or destruction could qualify as an armed attack. For example, the authors wonder whether an attack leading to the crash of a major international stock exchange—an action causing "severe, albeit not destructive" effects—would qualify as an armed attack.[75] The authors agreed that uses of force conducted in concert, which independently would not rise to the level of an armed attack, can be aggregated for their combined ability to rise to the level of an armed attack.[76] With regard to downstream consequences, if an attack against State A affects State C in a way meeting the scale and effects criteria, State C can respond so long as State C's response is proportional and necessary.[77] Additionally, the majority of the authors opined that it is immaterial as to whether the consequences were intentional.[78]

The Tallinn Manual incorporates the principles of necessity and proportionality in determining a legal response to an armed attack. It does so in accordance with conventional interpretations in international law.[79] Concerning necessity, the framework deems "non-forceful measures" as insufficient to "repel an imminent armed attack or defeat one underway."[80] Once force is considered necessary, the Tallinn Manual's proportionality constraint only limits "the scale, scope, duration, and intensity of the defensive response to that required to end the attack that has given rise to the right to act in self-defense."[81] No prohibition exists for the defensive response to be of the same nature as the armed attack.[82] Ultimately, the necessity and proportionality conditions are not tailored toward specific application to cyberspace. Instead, the framework employs a customary application without constraining factors.[83]

---

75 *Id.* at 343.
76 *Id.* at 342.
77 *Id.* at 344.
78 *Id.* at 343-44.
79 *Id.* at 348-50.
80 *Id.* at 349.
81 Nguyen, *supra* note 19, at 349.
82 *Id.* at 349.
83 *Id.* at 348-49.

The effects-based approach may appear to disqualify cyberattacks that are not severe enough to warrant an exception to the prohibition on the use of force.[84] However, upon consideration of the ramifications of such a regime, significant drawbacks arise. For instance, perverse outcomes can result from the tenuous relationship between the intended and realized consequences of a cyberattack, especially when compared to conventional weapons. A missile launched to destroy a satellite ground station will most likely create that desired effect or be intercepted beforehand. However, a cyber weapon employed to create a similar degradation of the ground station could have widely varying consequences. It may be successful, have little effect at all, or could cause other computer systems to be degraded in entirely unpredicted and unintended ways that would be unlikely in a kinetic attack. An effects-based framework may lead to a failure to address the bona fide motive of the aggressor. In determining whether an armed attack is underway, this information is vital because the exception to the use of force prohibition is to "maintain or restore international peace and security."[85] The true intent of an actor matters in determining whether to respond in self-defense because if an aggressor-state did not intend to commit an act of aggression violating another state's territorial integrity or political independence, there is no need to respond in self-defense.

To illustrate this approach, consider a hypothetical in the kinetic context: if the United Kingdom accidentally launched a missile at the United States, destroying a military base, it would be irrational for the United States to truly feel under attack once the unintended nature of the missile launch was known. Intent surely matters: the United States should not be granted the same justification to act in self-defense in this case compared to a scenario where the United Kingdom intentionally carried out the attack. Although its territorial integrity was breached in both cases, the United States should not be considered a victim of aggression that warrants the use of defensive force as if the United States were the victim of an intentional attack. While use of defensive force could be

---

[84] Michael Schmitt, '*Attack' as a Term of Art in International Law: The Cyber Operations Context* (4th Int'l Conf. on Cyber Conflict, 2012), https://ccdcoe.org/uploads/2012/01/5_2_Schmitt_AttackAsATermOfArt.pdf.

[85] U.N. Charter art. 51.

precluded in response to the United Kingdom under the principle of necessity, depending on it to disallow defensive force misconstrues the relationship between just cause and necessity in just war theory. As noted by political theorist Michael Walzer, "[a]ll aggressive acts have one thing in common: they justify forceful resistance. . . . Aggression justifies two kinds of violent response: a war of self-defense by the victim and a war of law enforcement. . . ."[86] But such a justification is intended to emerge from the just cause principle, rather than through the necessity principle in an ad hoc basis. In discussing Article 51's right to self-defense, Orend notes that "what is being defended against is aggression. . . ."[87] Thus, creating a legal regime that grants just cause to the United States as a result of the United Kingdom's accidental attack is contrary to the ethical precepts of just war theory because the United States was not wronged by an act of aggression. Yet, the Tallinn Manual's consequentialist regime does not account for this. Instead, it creates a system where countries, acting with aggressive intent, whose cyberattacks failed, are not punished for their actions. No matter how dire the consequences, a failed cyberattack is de facto authorized.[88] Ultimately, an effects-based model creates a perverse standard for the sanctioning and condemnation of actions; it ties "the legality of a [s]tate's cyber operations to the vagaries of chance without accounting for the significance of intent."[89]

Further complications arise from an effects-based framework because of the dependence on the victim-state's ability to repel or control the effects of an aggressor-state's cyberattack.[90] The aggressor-state's actions should not be evaluated on grounds of the victim-state's ability to defend itself. To illustrate the unreasonableness of this outcome, consider a domestic analogy: Person B attacks Person A with a bat. However, Person A has martial arts training and successfully defends herself from the attack. It would seem absurd if Person B's actions were legal because Person A escaped unharmed. While in a criminal proceeding, the relative

86 MICHAEL WALZER, JUST AND UNJUST WARS 52, 62 (1977).
87 OREND, *supra* note 7, at 34.
88 Nguyen, *supra* note 19, at 1122.
89 *Id.*
90 *Id.* at 1124.

severity of the punishment may be less—an aspect addressed in international law by the proportionality criterion—this mitigation does not mean that the aggressor's actions should be deemed legal. However, under an effects-based model, the legality of a cyberattack will be judged differently based on how vulnerable the victim-state is, analyzed through its investments in cyber defense and its ability to mitigate the effects of a cyberattack.[91]

In addition to the objectionable results of the effects-based model, the fundamental rationale behind its interpretation of Article 51 requires review. Michael Schmitt, the leading scholar in the development of the Tallinn Manual, posits that "Article 51 adopts an 'act-based' threshold using a specified type of action—an armed attack—rather than one based on particular consequences."[92] However, Schmitt argues that this can and must be reshaped to accommodate cyber weapons.[93] Despite the ICJ's Nuclear Weapons Advisory Opinion, which argues that the specific type of weapon used is of no import to Article 51, Schmitt opines that a cyber weapon is too "distant from the concept of 'armed'" because of the lack of "supporting elements typically associated with military assaults" and cyber weapons' destructive effect not resulting from a release of kinetic force.[94] Thus, to transpose cyberattacks onto the notion of armed attacks, cyberattacks require realized effects equivalent to the consequences of a conventional attack warranting a defensive response. Schmitt argues the following:

> [L]aw is about avoiding particular deleterious consequences. . . . So the right to resort to force in the face of an armed attack can be best appreciated as a right to do so when States face particular consequences that are severe enough to . . . use force. . . . [Armed attacks] in the cyber context can be interpreted as encompassing any acts that result in consequences analogous to those caused by the

91 *Id.*
92 Schmitt, *supra* note 84, at 287.
93 *Id.*
94 *Id.*

> kinetic actions originally envisaged by the term "armed attack."[95]

However, this conclusion is unsteady. Schmitt argues that the law seeks to avoid unfavorable consequences; thus, it follows that law should therefore be interpreted to avoid such consequences. In this way, the argument that cyberattacks should be evaluated not by the nature of the instrument used but by whether the instrument's effects satisfy the intent of Article 51 is sound. However, Schmitt conflates consideration of consequences in a general sense with a cyberattack's realized effects when he writes that it is the "result" that matters.[96] Interpreting law to avoid certain consequences does not mean that one must gauge acts based on the effectuated consequences. Schmitt has only proven that consequences should be evaluated in some capacity when considering defensive responses to cyberattacks; it would be just as allowable to review the intended consequences of a cyberattack to avoid "deleterious consequences" instead of reviewing the actualized effects to avoid such consequences. Thus, the Tallinn Manual's kinetic equivalence test has merit only up to the point of considering the consequences of the cyberattack.

Moreover, the ICJ's judgment in Nicaragua illustrates how the Tallinn Manual's adoption of an effects-based regime lacks grounding in international law. When evaluating the actions of the United States taken against the Nicaraguan government, the ICJ only considered the intent of the United States—to "secure a change of government policies"—in determining whether the United States unlawfully infringed upon Nicaragua's sovereign rights of territorial integrity and political independence.[97] The court opined:

> It appears . . . [clear] that the United States intended, by its support of the contras, to coerce the Government of Nicaragua in respect of matters in which each State is permitted, by the principle of State sovereignty, to decide freely. . . . The Court has

---

95 *Id.*

96 *Id.*

97 Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 241 (June 27).

> only examined the intentions of the United States Government so far as they bear on the question of self-defense.[98]

In determining whether the principle of non-intervention was breached, it was the intent that mattered, not the actualized results. While the Court was concerned with unlawful intervention instead of an armed attack, its holding can be insightful because both interventions and armed attacks are infringements upon a state's rights to territorial integrity and political independence. Since consideration of intent is needed to determine whether an unlawful intervention has occurred, intent must also factor into an armed attack determination—a violation of state sovereignty in another form. In essence, although the ICJ's holding concerned non-intervention, the Court's fundamental concern was whether there had been a breach of Nicaraguan sovereignty. When considering a similar method through which a breach of sovereignty may occur, it would be irrational to apply an antithetical approach. Yet, such a conclusion is contradictory to the Tallinn Manual, which states that "if a cyber operation that is designed to result in consequences breaching the sovereignty of another [s]tate fails, for instance due to effective defensive measures or because the operation was flawed, the latter's sovereignty has not been breached."[99] Applied to the cyber domain, an effects-based regime for answering questions of self-defense, such as that proposed in the Tallinn Manual, lacks substance compared to how related contraventions of sovereignty are approached in international law.

The Tallinn Manual also proffers several criteria meant to assist in evaluating whether a cyberattack can be classified as a use of force, including its immediacy, directness, invasiveness, and measurability. However, it has been noted that these characteristics are quite malleable and can be used to argue for a cyberattack qualifying as a use of force, an armed attack, or neither.[100] Ultimately,

---

[98] *Id.*

[99] The Tallinn Manual, *supra* note 15, at 24.

[100] *See* Oona Hathaway et. al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 847-48 (2012).

they are more likely to be used as tools for justification of a certain political agenda rather than helpful guidance for decision-makers.[101]

Despite the unsatisfactory effects-based regime and the malleability of its provided distinguishing factors, the Tallinn Manual has laudable aspects. First, not only is a kinetic equivalence test grounded in international law, but it is also a strong analogical tool for determining when a state may respond in self-defense because of the lack of an established definition for armed attacks in international law and cyberspace.

Second, the Tallinn Manual's acknowledgment that the consequences of a cyberattack can be spread among a variety of states due to the inherent interdependence of the cyber domain allows for any affected states to respond in a necessary and proportional manner. This essentially allows for State A, whose infrastructure depends on a control system in State B, to respond in self-defense should State C launch a cyberattack against the control system in State B's territory causing consequences in State A that are equivalent to a kinetic attack. Disallowing State A to respond, who is substantially affected,[102] negates the purpose of Article 51 of allowing any affected state to protect itself.

Finally, the aggregation of individual cyberattacks falling below the threshold of an armed attack is noteworthy because the use of the term "cyberattack" should not be conflated with an Article 51 armed attack. Debates during the drafting of the UN Charter dealt with the idea of an armed attack in terms of aggressive action in general, rather than in reference to a specific utilization of a weapon.[103] Thus, the interpretation of an armed attack to include multiple instances of uses of force in the cyber domain is congruent with the intention of Article 51 and does not create an unnecessary restriction limiting a victim-state's ability to respond to aggression.

---

101 *Id.*

102 This article's use of "trivial" intends to refer to cyberattacks that cause only irritation or inconvenience to the victim-state.

103 *See* RUYS, *supra* note 13, at 64.

The Tallinn Manual's framework for analyzing cyberattacks ultimately fails to be a satisfactory model because of its malleable, effects-based foundation that lacks grounding in international law. That the legality of a cyberattack depends on its inherent unpredictability and the investments and cyberspace dependency of the victim-state is unacceptable. Ultimately, intent must be considered in a coherent just cause framework.

2. Intentional Damage to Cyber-Physical Systems

This approach attempts to rectify the pitfalls associated with effects-based models for just cause by incorporating an intent-based condition while working to prevent the framework from becoming too permissive by limiting an armed attack to only constitute "irreversible disruption or physical damage to a cyber-physical system [(CPS)]."[104] The adoption of the CPS approach was intended to prevent a breach of international peace for operations not reaching Nicaragua's scale and effects standard and instead causing "mere disruption of service or functionality, with reversible and non-permanent results."[105] If a cyber weapon targets a computer system not controlling a physical component, this approach classifies the effects as too trivial to warrant designation as an armed attack because of its reversibility and perceived lack of severity.[106] In essence, this framework acts as an intent-based application narrowed to include only destructive or injurious effects using a target-focused standard. The approach only considers matters of just cause, leaving proportionality and necessity unaddressed and implying a perceived ability to satisfactorily evaluate just cause independent of the other principles.[107]

The model frames its applicability around the requirement for a cyberattack to intend to damage a CPS because it dissuades attacks that cause the "most damage"—irreversible and physical in nature.[108] However, the assertion that physical and irreversible effects are key

104 Nguyen, *supra* note 19, at 1125.
105 *Id.*
106 *Id.*
107 *See* Nguyen, *supra* note 19, at 1079, 1125-29.
108 *Id.* at 1128.

factors in determining whether a country has the right to use force to defend itself is an antiquated remnant from conventional warfare.

To illustrate the inapplicability of these restrictions, consider the 2007 Estonian Distributed Denial of Service (DDoS) cyberattack. Attributed to pro-Russian groups, the three-week attack targeted computer systems of the Estonian government, political apparatus, financial sector, and press, among other online services.[109] Meant primarily as "an act of communication," the attacks were intended to be a show of force by Russia against Estonia.[110] The attacks had a crippling effect on targeted sectors, such as freezing financial transactions and degrading communication inside the government.[111] It was the first time a cyberattack threatened the national security of an entire state;[112] Estonia suffered billions in damages.[113] Yet, under the CPS-focused approach, DDoS attacks of this nature would not qualify as armed attacks; despite their crippling nature, they cause no irreversible, physical damage.

The necessitation for physical damage largely rests upon the assertion that physical damage is worse than damage to internet systems.[114] However, the effects from the Estonian DDoS attack illustrate that the alleged connection between the two in severity is unfounded, particularly as global dependency on computer systems continues to rise.[115] Following the cyberattack, the Estonian Defense Minister compared the DDoS infrastructure blockade to a naval

---

109 JAMES PAMMENT ET. AL., HYBRID THREATS: 2007 CYBER ATTACKS ON ESTONIA. 52, 53 (2019).

110 *Id.* at 68.

111 *Id.* at 66; Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, THE GUARDIAN (May 16, 2007), http://www.guardian.co.uk/world/2007/may/17/topstories3.russia. ("The main targets have been the websites of: the Estonian presidency and its parliament; almost all of the country's government ministries; political parties; three of the country's big news organisations; two of the biggest banks; and firms specializing in communications.")

112 ALLISON RUSSELL, CYBER BLOCKADES 70 (2014).

113 PAMMENT ET AL., *supra* note 109, at 53.

114 *See* Nguyen, *supra* note 19, at 1127.

115 *See* RUSSELL, *supra* note 112, at 71.

blockade,[116] an action considered to be a use of force under Article 42 of the UN Charter.[117] This comparison is not novel as the similarities between the two have been previously observed:

> Naval blockades prevent the transport of people and products into the target country or area and may paralyze an economy. In the past, where intercontinental communication was largely by ship, a blockade would keep out information as well. An information warfare attack may also make transport of people and products impossible, paralyzing an economy, and it too may block the spread of information.[118]

This equivalence surely describes the crippling effects felt by the Estonian economy. But because the effects were not physical, no response would be warranted under the CPS framework. However, not only can the effects of a cyberattack be similar to a blockade, the effects of a cyberattack may be even more potent as today's economies are more dependent on computer systems than on maritime shipping in the past.[119] When the effects of cyberattacks are directly analogous to actions that may warrant a defensive response, and where such effects may be more damaging to a state than physical ones, the readiness to conclude that physical damage is the a priori standard for classification as an armed attack. However, this view fails to account for the dependence of modern states on cyber

---

[116] Nato Parliamentary Assembly, *NATO And Cyber Defence,* at ¶ 59, 173 DSCFC 09 E bis (Nov. 24, 2009).

[117] U.N. Charter art. 42. The U.N. Security Council is authorized to institute a naval blockade should "actions not involving the use of armed force" be inadequate, to include the interruption of economic relations and the severance of diplomatic relations. Furthermore, invocation of Article 42 has been used when urging the UN Security Council "to take all necessary measures, including the use of force" to restore international peace and security. U.N. Charter art. 42, Supp. no. 4. Thus, the designation of a naval blockade as a use of force is coherent.

[118] LAWRENCE GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW 19 (1998).

[119] OWENS ET AL., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 260 (2009).

systems. Essentially, degradation of computer systems is no longer an annoyance but rather a vital aspect of modern economies. The protection of such computer systems is of importance on par with physical systems conventionally considered to be crucial elements of a state's sovereignty and jurisdiction; modern policy must take this into account.

The 2007 Estonian attack was reversible in the sense that, once the attack was concluded, functionality to affected systems was restored. However, because of the nature of the attack, the degradation in capability was enduring unless changes were made either by increasing resilience to the network or ending the attack.[120] Yet, the CPS approach considers lasting effects solely in the material domain, where irreversible attacks—permanent imprints on the physical world—predominate. Ultimately, this precondition for the intended effects of an attack to be irreversible attempts to transpose a conventional measurement of damage to an atypical weapon.

The necessitation of irreversible damage rests upon the requirement for physical repair or replacement of an affected target which implies such damage is nontrivial and likely associated with consequences infringing upon state sovereignty.[121] Cyberattacks certainly can have analogous consequences, but they can also satisfy the requirement for repair or replacement. Although cyberattacks may not always impart physical damage, they nevertheless may require reversal in some form. In the case of a DDoS attack, a hardening against the attack or its conclusion at the hands of the aggressor is needed to reverse the damage. Further, a malware attack may require cyber professionals to detect, eliminate, and restore capabilities to affected computer systems—just as irreversible physical damage may require laborers to repair or replace a damaged physical object.[122]

---

120 *See* PAMMENT ET AL., *supra* note 109, at 59.

121 *See* Nguyen, *supra* note 19, at 1127.

122 *See* Robert Fanelli, *Cyberspace Offense and Defense*, 15 J. INFO. WARFARE 53, 58 (2016).

While the irreversible standard seeks to restrict fleeting uses of force from rising to the level of an armed attack,[123] it ignores the fact that cyber weapons can maintain characteristics analogous to what makes physically irreversible damage undesirable—an enduring nature causing deleterious effects. Creating a requirement for cyberattacks to cause irreversible effects prescribes an antiquated delineation that fails to account for the nature of computer systems. In the case of the Estonian DDoS attack, it would be faulty to claim that, had the attack continued or worsened, the crippling of a state's most vital industries could not allow for a defensive response because the attack's effects were not physically irreversible. Instead of a proscription on reversible attacks, a requirement for cyberattacks to be intransient would prevent evanescent attacks from rising to the level of an armed attack while instituting a more thorough condition for encompassing lasting cyberattacks infringing upon a state's sovereignty in a non-physical way.

Although this framework attempts to rectify the shortcomings of the Tallinn Manual's approach by proffering an intent-based regime, the current landscape of cyber warfare means the requirement for armed attacks to exclusively include physically irreversible cyberattacks is too constricting to determine when defensive use of force is warranted.

III. A NEW FRAMEWORK

To create a framework ameliorating the difficulties presented above, it is necessary to take a new approach incorporating an aspect of the jus ad bellum that has largely not been applied to the cyber domain: proportionality. As the principle of just cause has claimed much of the discussion surrounding cyberattacks, consideration of proportionality remains underappreciated. While the Tallinn Manual addressed the nuances of cyberwarfare in discussions of just cause, it approached proportionality in a cursory manner. And, in the case of the intent-based CPS-focused approach, a distinct evaluation of principles other than just cause was considered unnecessary to create a coherent framework for jus ad bellum in cyberspace.

---

123 Nguyen, *supra* note 19, at 1127.

By moving away from these narrowly delineated divisions and instead approaching jus ad bellum considerations with just cause and proportionality principles tailored to the cyber domain, a new approach can better address the challenges presented by the unconventional nature of cyberattacks. This new theory accounts for both intent and effects while remaining flexible enough to accommodate both physical and non-physical cyberattacks. By addressing concerns over permissiveness in both just cause and proportionality, the framework limits malleability while providing meaningful latitude for responding to a cyberattack.

A. Just Cause: Intent-Based Kinetic Equivalence

For establishing just cause in this new framework, an intent-based regime should be adopted for multiple reasons. First, this regime avoids the illogical outcomes presented by an effects-based approach.[124] Second, the ICJ's Nicaragua judgment, by undermining the effects-based framework, buttressed the adoption of intent as a critical factor in determining whether defensive action is justified.[125] Finally, evidence from customary practice indicates that states analyze intent in evaluating the presence of an armed attack. For instance, because of the "generally supportive attitude" of states following the U.S. military operation against the Iraqi intelligence headquarters, one can infer that a failed attempt to assassinate former President George H.W. Bush qualified as an armed attack.[126] A similar example arises in the 1964 attack against the Harib Fort in Yemen by British forces. Although the raid was condemned as a disproportionate use of force, a British defensive response of some kind was deemed justifiable by states despite Yemeni forces only causing the death of a "few precious camels."[127] A final example arises from an invocation of Article 51 by the United States to warrant the downing of two Libyan aircraft in the Gulf of Sidra in response to an alleged "unprovoked

---

124 *See supra* notes 84-91 and accompanying text.

125 *See supra* notes 97-99 and accompanying text.

126 RUYS, *supra* note 13, at 153; *see* U.N. SCOR, 48th Sess., 3245th mtg., 3, U.N. Doc. S/PV.3245 (Jun. 27, 1993).

127 RUYS, *supra* note 13, at 153; *see* U.N. SCOR, 19th Sess., 1106th mtg. § 67, U.N. Doc. S/PV.1106 (Apr. 2, 1964).

attack" by such aircraft.[128] While the American aircraft went unharmed, the intent to harm was dispositive.

Reasonably foreseeable outcomes arising from the cyberattack must also be considered. Although a specific test for determining reasonably foreseeable outcomes is beyond the scope of this article, it must at least include effects that could be objectively considered "natural and probable."[129] The inclusion of foreseeable effects is underpinned from both academic authorship and customary practice. In discussing which attacks would meet the armed attack threshold, the scholar Yoram Dinstein argues that what matters is whether the attack was "liable to produce such consequences," rather than the casualties or physical damage caused.[130] Furthermore, regarding whether small-scale conventional military actions can qualify as armed attacks, customary practice has indicated that the capability for destruction is required alongside effectuated destruction.[131]

1. The Armed Attack Threshold

This intent-based regime, which considers reasonably foreseeable consequences, mandates the consideration of many cyber operations previously discounted under an effects-based approach. Thus, it becomes vital to narrow these to include only those with the scale and effects of sufficient gravity to warrant an armed attack determination. To do so, the kinetic equivalence test employed in the Tallinn Manual will be adopted.[132] By providing an avenue for comparing cyberattacks to conventional uses of force, a variety of

---

[128] RUYS, *supra* note 13, at 154; *see* Steven Ratner, *The Gulf of Sidra Incident of 1981: A Study of the Lawfulness of Peacetime Aerial Engagements*, 7 YALE J. INT'L. L. 59, 76 (1984).

[129] *See* People v. Medina, 46 Cal. 4th 913, 920 (2009). While this is a criminal case occurring in a U.S. court, the presented standard could be usefully applied to international cyber law.

[130] DINSTEIN, *supra* note 51, at 193.

[131] RUYS, *supra* note 13, at 155. The cited analysis solely focused on conventional, terrestrial military action. It would be unlikely for the actions discussed by the author to lack intent to harm; therefore, explaining the author's bifurcation between effects and liable effects.

[132] *See supra* note 95 and accompanying text.

cyberattacks can be measured not by the means through which they accomplish their effects but by their intended and foreseeable effects. While the Tallinn Manual deferred as to whether the kinetic equivalence test should consider only destructive effects or all effects, the foregoing discussion illustrates why only considering destructive effects is inappropriate for the current environment.[133] Instead, all effects should be considered—including consequences that are physical and irreversible in nature in addition to those that may cause economic damage,[134] degrade a government's ability to carry out its duties, or cripple institutions upon which life depends.

However, before the kinetic equivalence test can be applied in determining whether a cyber operation has risen to the level of an armed attack, the operation must have risen to a use of force. To answer this question, the Tallinn Manual proffers numerous characteristics of a cyber operation, including military character, measurability of effects, invasiveness, and directness. Although nebulous,[135] considering a variety of qualities appears an appealing starting point. Yet, this approach conflicts with the intent of Article 2(4) and its prohibition of the use of force. The concept of state sovereignty, established in the 1648 Peace of Westphalia, created a right to autonomy—beyond the power of others to interfere.[136] To preserve sovereignty, states must have certain rights, especially political independence and territorial integrity.[137] The UN Charter affirmed this in Article 2(4).[138] In addition, the final clause of Article 2(4) disallows threats or uses of force "in any other manner inconsistent with the purposes of the UN Charter" and acts as a provisional statement to institute a "comprehensive ban against all

---

133 *See* discussion *supra* Part II.B.2.

134 Such economic damage would be more akin to the harm caused by a maritime blockade instead of an act of economic coercion such as flooding the global oil supply to reduce an oil-rich State's revenues.

135 *See supra* notes 100-101 and accompanying text.

136 FISHER, *supra* note 29; Legal Info. Inst., *Sovereignty*, WEX LEGAL DICTIONARY, https://www.law.cornell.edu/wex/sovereignty (last visited Jan. 13, 2023).

137 OREND, *supra* note 7, at 36.

138 Article 2(4) begins: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State. . . ." U.N. Charter art. 2, ¶ 4.

uses or threats of force, regardless of their impact or gravity."[139] Yet, as noted by scholar Thomas Franck, the clause forbidding actions contravening territorial integrity and political independence inadvertently allowed for the argument that the use of force prohibition did not include minor or fleeting actions that did not seriously contravene the victim-state's rights to sovereignty.[140] Ultimately, however, "such a reading of Article 2(4) is utterly incongruent with the evident intent" of its sponsors.[141]

For this reason, the criteria for determining a use of force qualification, such as military character, directness, or measurability of effects, is unnecessary. Article 2(4) did not intend to necessitate the creation of a distinction between cyber operations conducted by a military organization or delegated to another party under the supervision of the aggressor country. Nor should it be dispositive whether the operation's effects are immediately apparent or felt indirectly. Ultimately, the adoption of qualities for determining use of force, such as those found in the Tallinn Manual, is inconsistent with the intent of Article 2(4). Yet, because of the unconventionality of cyber operations, there must be a benchmark for establishing when a cyber operation qualifies as a use of force. Here, the kinetic equivalence analogical tool again proves useful. Rather than attempting to specify characteristics of a cyberattack to determine whether a cyber operation qualifies as a use of force, comparing the effects of the cyber operation to those of a kinetic operation is practical, consonant with actions in other domains, and adaptable to the evolution of general international law on the topic. Applying the kinetic equivalence test to the standards explicated in Article 2(4) simplifies use of force determinations while still addressing the fundamental justification for the Tallinn Manual's adoption of characteristics such as invasiveness, directness, and military character.

Ultimately, two conditions emerge that begin to establish just cause. First, a cyberattack warranting a use of force designation will have intended or reasonably foreseeable effects rising to the level of a

---

139 *Id.*; RUYS, *supra* note 13, at 57.

140 THOMAS FRANCK, RECOURSE TO FORCE: STATE ACTION AGAINST THREATS AND ARMED ATTACKS 12 (2002).

141 *Id.*

use of force by being equivalent to an illegal, kinetic use of force violating the victim-state's territorial integrity or political independence, or in any other manner inconsistent with the UN. Second, if a use of force determination has been made, the kinetic equivalence test can then be applied to determine whether the cyberattack rises to the level of an armed attack. This is encapsulated in the following condition: the intended or reasonably foreseeable scale and effects, if rising to the level of a use of force, will be nontrivial and of sufficient gravity in such a way as to be considered equivalent to an armed attack in the kinetic domain.

2. The Intransience Condition

The criteria established thus far requires a further condition addressing the possible fleeting nature of cyberattacks. It could be the case that the intended and foreseeable effects of a cyberattack indisputably rise to the level of an armed attack yet are only transitory and pose little serious risk to the victim-state. This outcome was sought to be avoided in the preceding approaches by evaluating effects for their irreversible or destructive nature. Although the irreversible and destructive standards are antiquated, the endurance of the cyberattack's effects must still be considered. To violate the use of force prohibition, the aggressive action must ultimately pose a risk to the victim-state's ability to exercise its foundational rights. In other words, the requirement for a cyberattack's effects to be lasting arises to ensure just cause is only granted in cases where the attack is more than a de minimis threat to the victim-state. Accordingly, an additional condition for establishing just cause must be that the intended, reasonably foreseeable, or realized effects are intransient such that not responding with defensive force would result in a significant and perceptible dereliction in the victim-state's rights to political independence and territorial integrity.

While the preceding conditions only considered intended and foreseeable effects, the clause's inclusion of realized effects is another way it addresses unintentional consequences. This inclusion allows for evaluation of whichever effect is more serious, creating a more flexible framework for evaluating cyberattacks. All cyberattacks warranting defensive force must first have intended or reasonably

foreseeable effects comparable to those of an equivalent armed attack. If the standard for an armed attack is reached, the intended or otherwise realized effects are evaluated for their intransient character. The benefits of this arrangement can be illustrated in a hypothetical: The cyberattack against State A is intended to cause severe damage to State B, indisputably rising to the level of an armed attack. However, the cyberattack influences the targeted computer system in unexpected ways, creating severe and intransient, yet unintended, effects. It would be irrational to disallow State B from responding to State A on the grounds that State A had malicious intent to harm but, by chance, the realized effects manifested in an unforeseeable manner. Otherwise, immunity would be ipso facto provided to State A despite the presence of a design to cause deleterious consequences and the harm caused to State B by not responding. Moreover, if only the realized effects were considered, the victim-state would be unduly restrained should the actual effects prove unable to be accurately gauged. The ability to reference intended, foreseeable, and realized effects provides the most complete way to address the intransience of a cyberattack.

3. Additional Considerations

Further conditions that should be considered when establishing just cause can be drawn from the Tallinn Manual.[142] This includes the aggregation of individual uses of force in the cyber domain which, despite individually falling below the threshold of an armed attack, warrant self-defensive force when aggregated. In addition, the new framework must provide states affected in an indirect manner by the intended consequences the right to evaluate such effects for their warranting of defensive use of force.

Attention must also be paid to actions taken by non-state actors. Following Al Qaeda's 9/11 attacks on the United States, the UN Security Council adopted resolutions furthering an interpretation of the UN Charter, traditionally construed to only incorporate actions from one state against another, to allow defensive force

142 *See* discussion *supra* Part II.B.1.

against non-state actors.[143] For actors not directly an organ of a state, yet acting seemingly on its behalf, the state must maintain "effective control" of the actor to be vicariously liable, pursuant with Nicaragua.[144]

4. A Coherent Approach

Combining the preceding conditions, an original framework for establishing just cause begins to take shape. Just cause is established should a state, organization under the effective control of a state, or a non-state actor uses a cyber weapon or amalgamation of weapons as part of a broader attack against another state, provided the following are satisfied:

A. The intended or reasonably foreseeable effects, direct or indirect, rise to the level of a use of force when commensurate with an illegal, kinetic use of force violating the victim-state's territorial integrity or political independence, or in any other manner inconsistent with the purposes of the UN.

B. The intended or reasonably foreseeable scale and effects, if rising to the level of a use of force, must be nontrivial and of sufficient gravity to be considered equivalent to an armed attack in the kinetic domain; and

C. The intended, reasonably foreseeable, or realized effects must be intransient such that not responding with defensive force would result in a significant and perceptible dereliction in the victim-state's rights to political independence and territorial integrity.

This framework's merit is only sustained provided it can be successfully applied to hypothetical and historical scenarios. First, consider the variety of outcomes reaching the scale and effects standard, with consequences that include the following:

---

143 S.C. Res. 1368 (Sept. 12, 2001); S.C. Res. 1373 (Sept. 28, 2001).

144 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶¶ 64-65, 115 (June 27).

> [T]he infliction of substantial destruction upon important elements of the target [s]tate namely, upon its people, economic and security infrastructure, destruction of aspects of its governmental authority . . . as well as damage or deprivation of its physical element . . . and the use of force which is aimed at a [s]tate's main industrial and economic resources which results in the substantial impairment of its economy.[145]

These effects would qualify as a contravention upon a state's territorial integrity or political independence and therefore, under the kinetic equivalence framework, would satisfy the use of force and armed attack criteria. However, the intransience condition proves necessary by precluding cyber operations which may generate the consequences in an ephemeral manner. This approach to measuring effects, while beneficial in its ability to evaluate the intent-based kinetic equivalence approach, is only a tool. While some may attempt to create a regime around cyberattacks only affecting these outcomes,[146] such an approach fails to adapt to the diverse types of cyberattacks and the generally transformative nature of today's world; they cannot account for the possible fleeting nature of an attack.

Consider an example where a cyberattack intends to significantly degrade the functionality of an online stock exchange. Substantial economic damage would ensue, and billions could be wiped off the market. While the effects are not irreversible, it will take at least several days for functionality to be restored and damage to be repaired. The political independence of the affected State would be violated, as its ability to control financial decisions would be significantly impaired. Compare this to a physical example: a bomb is placed inside of a physical stock exchange in a major financial city. It is timed to only detonate at night where no casualties will be inflicted and will largely only damage servers integral to the operation of the exchange. The damage is irreversible, but, like the cyberattack, repairs will take days before functionality is eventually restored.

---

145 CONSTANTINOU, *supra* note 54, at 63-64.

146 ROSCINI, *supra* note 23, at 73.

In this hypothetical, the effects of the cyberattack are mitigated and the bomb is disarmed before detonation. While it would hardly seem reasonable to qualify the latter act as an act warranting a defensive response but not the former, only the approach suggested here may classify such a cyberattack as warranting self-defense. This conclusion is reached through consideration of the intended scale and effects, the example's implicit kinetic equivalence, and the reasonably foreseeable intransience of the cyberattack. Granting of just cause is unneeded as the various criteria of the jus ad bellum framework are not assuredly satisfied. However, the example demonstrates the usefulness of this model's approach to just cause by not summarily precluding a defensive response to a halted cyberattack against a critical, non-physical target. On the other hand, a cyber tool that legally manipulates securities exchanges in such a way as to hinder the economic success of the target nation would likely not presuppose a right to use defensive force because such an action appears to be an example economic coercion—an action deemed not to be a use of force.[147] The interplay between kinetic equivalence, intent, and intransience proves to be a flexible yet realistic way to evaluate cyberattacks.

The Stuxnet worm, under the intent-based kinetic equivalence model, would qualify as a use of force because the attack was a contravention of Iran's political integrity, and the resulting damage caused to the Iranian nuclear centrifuges would have reasonably been considered a use of force if the destruction had come from a conventional, kinetic attack.[148] However, while there is no consensus as to whether the attack met the scale and effects standard rising to an armed attack,[149] this indecisiveness could be ameliorated due to the lack of a bright line between use of force and an armed attack. Should the distinction between the two become more delineated, the proffered approach could adapt to the clarification. Thus, the intent-based kinetic equivalence framework aligns with both views concerning the cyberattack but is ultimately

---

147 Editors, *The Use of Nonviolent Coercion: A Study in Legality under Article 2(4) of the Charter of the United Nations* 122 U. PA. L. REV. 983, 991 (1974).

148 The conclusions herein regarding Stuxnet operate from the assumption that the attack was not otherwise justified.

149 The Tallinn Manual, *supra* note 15, at 341.

limited by international law's ambiguous standards.[150] In a similar vein, this approach, while shaped under the assumption that uses of force and armed attacks are discrete concepts, can be easily adapted to account for alternative interpretations of international law.[151]

Another example involves actions taken against Ukraine in 2022, where the Ukrainian government was warned by Microsoft Corporation that a "highly destructive form of malware in dozens of government and private computer networks in Ukraine . . . appeared to be waiting to be triggered."[152] The code was meant to appear as a form of ransomware—a cyber weapon that cripples a computer system's functions until a monetary demand is met—except there was no function accepting payment, leading to the conclusion that the malware was intended to cripple the affected computer systems indefinitely.[153] Despite the apparent intransient nature of the attack and clear intent to violate Ukraine's political independence, this article's approach would not grant Ukraine just cause. In this case, a Ukrainian use of force would be unacceptable because the cyberattack has not been activated and there is no guarantee that such an activation will ever occur—the potentiality for damage could exist indefinitely. Such a position is akin to a heightened state of readiness for conventional troops—the capability for immediate military action exists but escalation is not assured. Thus, while the triggering of the cyber weapon could qualify as an attack justifying a defensive response, in its inactivated state, such an action is unwarranted.[154]

None of the preceding examples involve a scenario where a state, acting with hostile intent, launches a cyberattack against a victim-state intending to cause mere inconvenience and irritation, where the actualized effects go far beyond what was intended, and are of a severity rivaling that of a highly destructive kinetic attack. Would the victim-state have the legal right respond to the aggressor,

---

150 *See supra* notes 38-40 and accompanying text.

151 *See supra* notes 45-46 and accompanying text.

152 David Sanger, *Microsoft Warns of Destructive Cyberattack on Ukrainian Computer Networks*, N.Y. TIMES (Jan. 16, 2022), https://www.nytimes.com/2022/01/16/us/politics/microsoft-ukraine-cyberattack.html.

153 *Id.*

154 This discussion assumes the criteria for preemption are unmet.

who is acting with hostile intent? In the case that the unintended effects were intransient and reasonably foreseeable, the victim-state may respond using defensive force under Article 51. However, if these effects were unforeseeable and not the result of knowing, willing, or negligent actions taken during the development of the cyber weapon, the planning of the mission, or the gathering of intelligence related to the attack, the victim-state does not have a right to use defensive force. Otherwise, it would be unreasonable and unfair to punish the aggressor for an outcome entirely out of its control. While the moral reprehensibility of the aggressor nation could cause some to reject this designation, this restraint is imperative for the coherence of just war theory. The compelling reason for maintaining jus ad bellum criteria is to avoid indiscriminate and unnecessary harm. Placing restraints on a defensive response should the consequences of a cyberattack be unforeseeable is necessary for the victim-state to avoid descending to the same morally corrupted level as the aggressor. Yet, it is important to note that the victim-state is not precluded from using other measures not rising to the level of a use of force, such as economic or political coercion, to deter the aggressor-state from future hostilities. This approach creates a useful balance between intent and unintended effects.

By simplifying the criteria to less malleable and abstract principles, considering the aggressor-state's intent rather than solely the realized effects, creating a forward-thinking method for addressing concerns over ephemeral attacks, and moving away from restrictive, target-based approaches, the intent-based kinetic equivalence model is the best suited for evaluating whether just cause is established considering a cyberattack. Yet, this is only a portion of what is needed to create a more cohesive jus ad bellum framework. Proportionality, often relegated as an easily applicable principle to the cyber domain, requires additional consideration in an intent-based framework.

B. Synthesized Proportionality

While the effects-based model for just cause is too restrictive and leads to deleterious outcomes when applied, the intent-based model for just cause, on its own, is too permissive; it fails to consider

the susceptibility of a state to the intended cyberattack. Therefore, the jus ad bellum principle of proportionality must be considered in a cyber-specific manner. Yet, scholarship on the proportionality of defensive responses to cyberattacks has largely focused on the jus in bello domain.[155] And the two models considered previously concluded that proportionality either did not need to be specifically addressed in creating a jus ad bellum framework or could utilize the standard means-end interpretation of proportionality in international law. By breaching this convention, a more complete framework for evaluating the jus ad bellum criterion in cyberspace can be established by synthesizing means-end proportionality alongside narrow proportionality.

As discussed in Part 1.A, the means-end approach seeks to limit the proportionality of the defensive response to one where the use of force is used insofar as the armed attack is halted and repelled.[156] In essence, the response is limited to avoid retributive attacks. However, the means-end approach, when combined with an intent-based framework for establishing just cause, leads to unsatisfactory outcomes. Consider a scenario where a cyberattack is conducted against a victim-state whose cyber defenses are virtually impenetrable. The severity and intransience of the attack establishes the right to just cause. Yet, the risk of deleterious effects to the victim-state is extremely small and the benefit gained from responding is slight. Furthermore, the principle of necessity is also satisfied in this scenario—the only way for the aggressor-state to cease its attack is to use force. It would be irrational not to constrain the actions of a state—inside jus in bello restrictions—as it attempts to repel the cyberattack or halt the aggressor-state from launching subsequent attacks. Such a response appears to be disproportionate, despite being warranted under the means-end approach.

Herein lies the difficulty with an intent-based just cause framework; in an effects-based model, the vulnerability of the victim-state is of little import because only successful cyberattacks are considered as a basis for just cause. However, because of the

---

155 *See supra* note 67.

156 RUYS, *supra* note 13, at 112.

deleterious outcomes resulting from an effects-based framework, the more permissive intent-based model must be adopted. As additional cyberattacks are considered, there is an increased possibility for disproportionate responses which the conventional means-end approach cannot ameliorate because it cannot, on its own, account for the risk posed to the victim-state. Therefore, an approach for addressing proportionality in cyberspace should only begin with a means-end foundation to prohibit retributive attacks; the objective for the defensive response to only be continued until the securing of the just cause is necessary to a proportional response.[157] The securing of "just cause" does not refer solely to the halting and repelling of an armed attack. Because of the importance of passive defense in combatting cyberattacks, active defense to counteract the effects of an attack may not be necessary or feasible. That the cyberattack was "ended" such that it was successful, defended against, or a partial combination of the two, should not preclude the victim from responding with defensive force if it is believed that the aggressor-state has both the capability and will to commit further violations of the victim-state's territorial integrity or political independence. Securing just cause involves halting and repelling an attack, ensuring that the aggressor-state no longer has the capability or will to commit future armed attacks against the victim-state. Inside of this means-end restraint, the benefits gained from a forceful response should not be dwarfed when compared to the universal costs. Due to the possible nebulousness of such a cost-benefit analysis, in what form should this determination manifest itself?

Narrow proportionality espouses the need for limits to a response in self-defense so that the benefits of ending the attack are

---

[157] In *Morality and War*, Orend questions whether responding in a domain other than cyberspace to a cyberattack is disproportional. OREND, *supra* note 7, at 177. The Tallinn Manual offers a convincing response when discussing proportionality: "It may be that the originator of the cyber armed attack is relatively invulnerable to cyber operations. This would not preclude kinetic operations to compel the attacker to desist, although they must be scaled to that purpose." The Tallinn Manual, *supra* note 15, at 349. Fundamentally, what matters in proportionality is not that the response is domain-dependent, a requirement that may unnecessarily restrict the victim-state. Moreover, such a restriction upon defensive responses to cyberattacks ignores cyberwarfare's ability to create effects equally deleterious to conventional attacks.

equal or greater than the projected costs. As discussed, states' susceptibility to a cyberattack should play a role in determining what defensive response is warranted. However, a competing interest is the severity of the intended effects. These two considerations oppose each other in evaluating the benefits of a response. On one end of the spectrum is an attack with a relatively minor intended effect and a very small chance of causing damage. On the other would be an indefensible attack with the intended effect of crippling a state's infrastructure. And in the middle of these two extremes lies a gray area, where a commensurate balancing between the intended effect and the risk to the victim-state and other vulnerable states must be attempted. As the intended effect becomes direr, a lower risk of success is needed to justify an equivalent attack. It would not be cogent to allow a state with an "impregnable" defensive apparatus that contained the effects of a cyberattack to respond in an equivalent manner as a state afflicted by an equally severe, but successful, cyberattack. A victim-state that suffers minimal damage gains little benefit from launching a retaliatory attack against an aggressor-state when their weapon is largely useless. Thus, while the victim-state may have just cause to use force in self-defense, the severity of such a response must be presumptively marginal. Ultimately, in establishing proportionality, the action should be continued until just cause is secured. But the universal costs of such a response must not be indiscriminate when compared to its benefits—calculated through an appraisal of the cyberattack's intended effects and the risk to the victim-state and other vulnerable states.

Although some believe that evaluating the act of aggression and the needs of self-defense together would be unfeasible,[158] such a framework has already been incorporated in conceptions of proportionality in domestic law. A combination of means-end and narrow proportionalities, originating in German administrative law, has been widely adopted in countries such as Canada and Israel.[159] Therefore, despite its absence in international law, its intuitiveness has led to incorporation in domestic legal regimes. Accordingly, the

158 Kretzmer, *supra* note 58, at 262.

159 *Id.* at 277-78.

argument that such an approach cannot be applied in the jus ad bellum tradition is tenuous.

For attacks that have some measure of success, the realized effects play a role in the determination of the risk to the victim-state and other states. Because of the nature of cyber warfare, passive defense is often the main avenue through which such attacks are mitigated.[160] Thus, the only way the risk to a victim-state can be determined is through a post hoc analysis, using the consequences of such an attack. For instance, if the intended effects were fully realized, or took a different form of similar severity,[161] the risk to the victim-state would be found to be of the highest order.

This balancing of risk to the victim-state and other vulnerable states and the intended severity of effects often does not provide a clear delineation as to whether an attack is proportionate. Instead, as often is the case with proportionality considerations, it will be clearer regarding whether an action is disproportionate.[162] Proportionality is meant to be a guide to decision-makers as a check before a defensive response is initiated—rather than a bright line. Although difficulties and complexities in this analysis are present, this does not render it futile. Although this assessment may be daunting, "it should be undertaken with due humility and in full recognition of those difficulties. But it is mistaken to argue that the politicians who make decisions of war and peace should be excused from assessing the consequences of their actions because of the practical difficulties involved."[163]

Consider a hypothetical example where a state with a relatively effective cyberattack defense apparatus is attacked by a cunning and well-funded enemy. The attack targets a satellite communications operations center and intends to bring the system offline. The attack is partially unsuccessful because of the country's

---

160 *See* Fanelli, *supra* note 122, at 60.

161 Including unintentional effects creates a responsibility for unintended consequences. Despite its difficulty to control the effects, an incentive to do so is created.

162 *See* RUYS, *supra* note 13, at 111-15.

163 FISHER, *supra* note 29, at 75.

defenses but does manage to degrade some of the center's capabilities in a nontrivial and lasting, though impermanent, manner. The consequences of the attack illustrate to the victim-state that not only does the aggressor-state have the intent to cause significant harm, but also that there is a credible risk of such harm occurring. Thus, the victim-state is provided with just cause to respond using force and in a manner, including kinetic measures, to defend itself against the threat. However, such force should be limited in such a way as to restrict the most deleterious measures because of the limited risk to the victim-state—despite severe intended effects. For instance, tranches of operations posing the highest risk to civilians or dual-use infrastructure would be normatively prohibited.

Through this approach, the permissiveness of a response to a cyberattack is addressed across both the just cause and proportionality criteria, rather than solely within the principle of just cause and to the detriment of the overall coherence of cyber-specific jus ad bellum considerations. Furthermore, this framework creates a spectrum of allowable conflict with varying degrees of severity. This allows a more realistic way for states to legally respond to attacks by placing broad restraints on the intensity of the defensive response without overly restricting it through an exclusively narrow proportionality regime.

IV. CONCLUSION

The Stuxnet virus illustrated to the world how a cyber weapon could infiltrate a computer network system and inflict precise, physical damage. Similarly, the 2007 Estonian DDoS attacks illustrated the general dependency on computer systems and the potential such a weapon has to cripple a state's governmental and financial infrastructure without inflicting physical damage. Scholars have proffered various ways in which the broad scope of cyberattacks can be evaluated within Just War Theory's jus ad bellum tradition. However, these frameworks, often focusing on applying just cause to the cyber domain, cannot adequately address the multitude of ways in which cyber weapons can compromise a state's territorial integrity or political independence. This article proposed a new analytical model providing coherence and flexibility to create a foundation for future

policy. For the principle of just cause, this model moves away from a purely effects-based framework and rejects the antiquated requirement for physical damage. Furthermore, diverging from conventional practice, a cyber-specific method to evaluate proportionality is created by synthesizing two often-separated functional approaches. A complete outline of the proposed jus ad bellum regime is provided below.

A. The Jus Ad Bellum Framework for Cyberspace

Just cause is established should a state, a party under the effective control of a state, or a non-state actor:

A. Utilize a cyber weapon or amalgamation of weapons as part of a broader attack against another state;

B. Where the intended or reasonably foreseeable effects, direct or indirect, rise to the level of a use of force when commensurate with an illegal, kinetic use of force violating the victim-state's territorial integrity or political independence, or in any other manner inconsistent with the purposes of the United Nations;

C. Where the intended or reasonably foreseeable scale and effects, if rising to the level of a use of force, are nontrivial and of sufficient gravity to be considered equivalent to an armed attack in the kinetic domain; and

D. Where the intended, reasonably foreseeable, or realized effects are intransient such that not responding with defensive force would result in a significant and perceptible dereliction in the victim-state's rights to political independence and territorial integrity.

Should just cause be established, defensive force must be found to be necessary using the following criteria:

A. The need for the defensive response must be of last resort, where other means of redress would clearly be

futile, though not necessarily attempted before use of force is warranted;

B. The response should be focused only on targets involved in the armed attack; and

C. The response should be exercised with immediacy in anticipation of or during the cyberattack or during the course of a broader armed attack, seeking to distinguish actions of self-defense from unlawful reprisals.

If the proposed use of force is necessary and is publicly declared by a proper authority, it must also be proportional, evaluated through the proceeding considerations:

A. To avoid retributive actions, the defensive response should be continued until the just cause is secured, such that the cyberattack is halted and repelled and the aggressor-state no longer has the capability to commit future armed attacks against the victim-state.

B. Until Part A is satisfied, the universal costs of the response must be proportionate to its benefits, when calculated through a commensurate consideration of the cyberattack's intended effects and the risk to the victim-state and other vulnerable states.

International law of various kinds, including customary practice, will eventuate an accepted cyber law framework for determining the conditions under which a victim-state may resort to defensive force. Yet, the exponential increase of cyberattacks' importance in modern warfare reinforces the necessity of establishing these norms correctly and expeditiously.