THE FUTURE OF JUST WAR THEORY IN THE AGE OF CYBERWARFARE

DR. WASEEM AHMAD QURESHI*

ABSTRACT

Just war theory has developed and evolved over centuries into its present form. In modern times, the only justifications for war are state defensive purposes or United Nations Security Council (UNSC) authorization. The UN member states altered just war theory in order to foster the status quo and to maintain global peace and security. Yet, some countries find ways to justify their actions against weak states even in contemporary times. Some scholars and international organizations have produced concepts in just war theory that wrongfully justify the aforementioned conflicts, and over time these notions of "responsibility to protect," "humanitarian intervention," "pre-emptive and preventive self-defense," and the "unwilling or unable test" have emerged. These concepts have costs and are not justified. Since just war theory has continued to evolve and may be modified in the future, this Article examines the future of just war theory. To this end, this Article explores the aspects of information warfare (under just cause and self-defense), and the consideration of legitimate authority for nonstate actors, as supported by Caron Gentry.

* Advocate Supreme Court of Pakistan.

INTRODUCTION

Just war theory regulates warfare. Its application goes back centuries; its foundations laid by classical philosophers including Augustine and Grotius.[1] The classical formulation of just war theory has two parts: *jus ad bellum* and *jus in bello*. *Jus ad bellum* explains the just causes of wars and delineates when and how a war is justified,[2] while *jus in bello* regulates the actions and ways of fighting a war. The latter element is purely humanitarian, and seeks to limit excessive violence, as well as to protect innocent people during armed conflicts and wars.[3]

The theory has evolved dramatically over the past centuries,[4] such that its present form does not resemble its classical form. Yet, the fundamentals of the theory's nature have remained intact: protecting the innocent and seeking to limit violence in warfare. Modern just war theory propounds that states are only justified in initiating wars for defensive purposes or through authorization by the United Nations Security Council (UNSC).[5] Over the last few decades, however, there have been deliberate attempts by states to adapt just war theory in order to justify illegitimate wars. In consequence, jus ad bellum has seen scholastic movements in support of humanitarian intervention,[6] pre-emptive or anticipatory

---

1 Michael Farrell, MODERN JUST WAR THEORY: A GUIDE TO RESEARCH 173 (2013).

2 ICRC, *What Are Jus ad Bellum and Jus in Bello*?, (Jan. 22, 2015), https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0 [https://perma.cc/W6TY-6AP7]. *See also*, ICRC *Jus ad Bellum and Jus in Bello,* (Oct. 29, 2010), https://www.icrc.org/en/document/jus-ad-bellum-jus-in-bello [https://perma.cc/69HA-F5EZ]; Jasmine Moussa, *Can Jus ad Bellum Override Jus in Bello? Reaffirming the Separation of the Two Bodies of Law,* 90 INT'L REV. RED CROSS 963 (2008); François Bugnion, *Jus Ad Bellum, Jus in Bello and Non-International Armed Conflicts* ICRC (Oct. 28, 2004), https://www.icrc.org/en/doc/assets/files/other/jus_ad_bellum,_jus_in_bello_and_non-international_armed_conflictsang.pdf [https://perma.cc/UU5U-UDTD].

3 *See supra* note 2.

4 *See* Farrell, *supra* note 1, at 7–11.

5 U.N. Charter art. 2, ¶ 4, art. 39–51.

6 MARK GRY CHRISTIANSEN, *HUMANITARIAN INTERVENTION: LEGAL AND POLITICAL ASPECTS* (1999). *See also* Neba Ridley, NGWA, *The Rise and Decline of Humanitarian Intervention And Responsibility To Protect* ULUSLARARASI SOSYAL ARAŞTIRMALAR DERGISI 10 [J. OF INT'L SOC. RES.] 121 (Apr. 2017); Robert Kolb, *Note on Humanitarian Intervention*, 85 AFFAIRES COURANTES ET COMMENTAIRES [RICR] [CURRENT ISSUES AND COMMENTS] 119 (Mar. 2003); Şaban Kardaş, *Humanitarian Intervention: The Evolution of the Idea and Practice* VI(2) J. INT' L AFF. (2001); Watanabe Koji, *The Debate on Humanitarian Intervention, Humanitarian Intervention: The Evolving Asian Debate* JAPAN CENT. INT'L EXCH., 11–18, (2003), https://www.jcie.org/researchpdfs/HumInterv/human_watanabe.pdf [https://perma.cc/686H-9YGY]; TAYLOR B. SEYBOLT, HUMANITARIAN MILITARY INTERVENTION THE CONDITIONS FOR SUCCESS AND FAILURE (2008); Jana Dadova, *The Legality of Humanitarian Intervention without*

preventive self-defense,[7] the responsibility to protect,[8] and the unwilling or unable test.[9] Although these concepts have been put forth as a part of just war theory, they do not fit into the theory because just war theory prohibits the use of force.

In order to adapt just war theory in a post-war period, scholars recommend including the notion of *jus post bellum* within the ambit of just war theory for post-war scenarios—that is, the morality of the termination phase of war—to reflect modern circumstances.[10] The notion of jus post bellum[11] has recently become a popular topic of discussion among scholars, including Brian Orend.[12] Orend argues that the application of just war theory should not terminate when a war ends; instead, just war theory should continue to apply to protect the rights and sovereignty of defeated states after a war is over.[13] Likewise, James M. Dubik argues that although jus in bello deals with the humanitarian laws of war to restrict violence against innocent people, there is still a missing piece.[14] He argues that jus

---

UN Security Council Authorization, RESEARCHGATE (May 2016); TOM RUYS, ARMED ATTACK AND ARTICLE 51 OF THE UN CHARTER: EVOLUTIONS IN CUSTOMARY LAW AND PRACTICE 107 (2010).

7 *See* Patrick Kelly, *Preemptive Self-Defense, Customary International Law, and the Congolese Wars*, E-INTERNATIONAL STUDENTS (Sept. 3, 2016), https://www.e-ir.info/2016/09/03/preemptive-self-defense-customary-international-law-and-the-congolese-wars [https://perma.cc/9DMS-BB9T]. *But see* Andrew Garwood-Gowers, *Pre-Emptive Self-Defence: A Necessary Development or the Road to International Anarchy*, 23 AUS. Y.B OF INT'L. L. 51 (2004). *See also* Daniel Bethlehem, *Principles Relevant to the Scope of a State's Right of Self-Defense against an Imminent or Actual Armed Attack by Nonstate Actors*, 106 AM. J. INT'L L. 770 (2012); *Why Preventive Self-Defense Violates the UN Charter*, OPINIOJURIS (Mar. 7, 2012), http://opiniojuris.org/2012/03/07/why-preventive-self-defense-violates-the-un-charter [https://perma.cc/53Q4-PZUC].

8 Sandra Fabijanić Gagro, *The Responsibility to Protect (R2P) Doctrine*, III (1) INT'L. J. SOC. SCI. 63 (2014). (discussing Kosovo intervention without UNSC authorization). *See also*, David Chandler, *Unravelling the Paradox of the Responsibility to Protect*, 20 IR. STUD. INT'L AFF. 27 (2009).

9 Ashley S. Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extra-Territorial Self-Defense*, 52 VA. J. INT'L L. 483 (2012). *See also*, Waseem Ahmad Qureshi, *International Law and the Application of the Unwilling or Unable Test in the Syrian Conflict*, 11 DREXEL L. REV. 61 (2018) [hereinafter *Unwilling Test in Syrian Conflict*]. *See also*, Waseem Ahmad Qureshi, *Examining the Legitimacy and Reasonableness of the Use of Force: From Just War Doctrine to the Unwilling-Or-Unable Test*, 42 OKLA. CITY U. L. REV. 221 (2018) [hereinafter *Reasonableness of Use of Force*].

10 HELEN FROWE & GERALD LANG, HOW WE FIGHT xiii (2014). *See also*, David Fisher, MORALITY AND WAR: CAN WAR BE JUST IN TWENTY-FIRST CENTURY? 79–80 (2011).

11 *See supra* note 10.

12 Brian Orend, *Jus Post Bellum*, 31 J. SOC. PHILOSOPHY 117 (2000).

13 *See supra* note 10.

14 James M. Dubik, JUST WAR RECONSIDERED 7–26 (2018).

in bello only applies to warfare in action at the tactical level, where military necessity and collateral damage can justify violations of humanitarian law in particular situations.[15]

Scholars should consider adjusting jus in bello to include monitoring wars at the strategic level, where the real game-changing plans are made.[16] By doing this, people who are truly responsible for the aggressions of war and for ordering the killing of innocent people could be held responsible for their actions.[17] Take, for example, the tactics of fourth[18] and fifth generation warfare,[19] cyberwarfare,[20] and hybrid wars,[21]

---

[15] *Id.* at 13.

[16] *Id.* at 22.

[17] *Id.* at 26.

[18] William S. Lind, *The Four Generations of Modern War* (June 11, 2004), https://www.lewrockwell.com/2004/06/william-s-lind/the-four-generations-of-modern-war/ [https://perma.cc/B5ML-X6CB]. *See also*, William S. Lind, *Understanding Fourth Generation War*, Military Rev. (Sept–Oct 2004); Thomas X. Hammes, The Sling and the Stone: On War in the 21st Century 208 (2004); Thomas X. Hammes, Insurgency: Modern Warfare Evolves into a Fourth Generation 214 STRATEGIC FORUM (Jan. 2005); Harold A. Gould & Franklin C. Spinney, *4GW is Here!* SMALL WARS J. (2001), https://smallwarsjournal.com/documents/4gw.htm [https://perma.cc/HTN4-MTTJ]; Albert A. Nofi, Recent Trends in Thinking about Warfare 87 (2006).

[19] Daniel H. Abbott, *Dreaming Fifth Generation War*, *in* THE HANDBOOK OF 5GW (2010). *See also* Adam Herring, *Working Definition*, *in* THE HANDBOOK OF 5GW (2010); Mark Safranski, *Unto the Fifth Generation War*, *in* THE HANDBOOK OF 5GW (2010); Curtis G. Weeks, *On the Barnettian 5GW*, *in* THE HANDBOOK OF 5GW (2010); RYAN BURKE, MICHAEL FOWLER, & KEVIN MCCASKEY, MILITARY STRATEGY, JOINT OPERATIONS, AND AIRPOWER: AN INTRODUCTION 142 (2018); DANIEL H. ABBOTT, THE HANDBOOK OF 5GW 11–25 (2010).

[20] Michael Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, 56 VILL. L. REV. 569, 604 (2011). *See Also*, FRED KAPLAN, DARK TERRITORY: THE SECRET HISTORY OF CYBER WAR 161 (2016); HEATHER H. DINNISS, CYBER WARFARE AND THE LAWS OF WAR (2012); MICHAEL SCHMITT, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO THE CYBER WARFARE (2013); Pete Warren, *State-Sponsored Cyber Espionage Projects Now Prevalent, Say Experts*, THE GUARDIAN, Aug. 30, 2012; Dave Lee, *Flame: Massive Cyber-Attack Discovered, Researchers Say*, BBC NEWS, May 28, 2012; Ben Saul & Kathleen Heath, *Cyber Terrorism*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBER SPACE (Nicholas Tsagourias & Russell Buchan eds., 2015); Hamadoun Toure, *Cyberspace and the Threat of Cyberwar*, *in* THE QUEST FOR CYBER PEACE 7–13 (2011).

[21] James K. Wither, *Making Sense of Hybrid Warfare*, 15(2) CONNECTIONS Q. J. 73, 76 (2016). *See Also*, Swedish Defence University Conference Proceedings, Karl Hickman et al., Hybrid Threats and Asymmetric Warfare: What to Do?, 20–21 (Feb. 15, 2018) https://www.diva-portal.org/smash/get/diva2:1186265/FULLTEXT01.pdf [https://perma.cc/9M6M-H5D5]; Patrick J. Cullen & Erik Reichborn-Kjennerud, *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*, 12 (2017) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf [https://perma.cc/8E8T-EYAZ];The CANSOFCOM Professional Development Centre, Colonel Bernd Horn, On Hybrid Warfare, 16 (2016) http://publications.gc.ca/collections/collection_2017/mdn-dnd/D4-10-19-2016-eng.pdf [https://perma.cc/3RR5-QS8Q];Manon van Tienhoven, Identifying Hybrid Warfare, 13 (2016)

in which those who initiate violence deliberately target nonmilitary persons so as to destabilize nations. Likewise, non-state actors (NSAs) are employed in asymmetric warfare to avoid attribution and retribution.[22] If the conventional approach to enforcing humanitarian law will be undertaken in such asymmetric settings to hold war criminals responsible, it will be difficult for international courts to prosecute the upper hierarchies of militaries for violations of humanitarian laws. NSAs could slip through the cracks because humanitarian laws target the tactical level and not the strategic level.[23] However, if humanitarian laws, as argued by Dubik, are revised in such a way that they are applicable at the strategic level of warfare, then the decision makers and plotters can also be held liable for schemes of aggression and for humanitarian law violations committed by their agent-NSAs.[24]

Similar to the propositions of introducing the notion of jus post bellum[25] and including the monitoring of wars at strategic level,[26] Caron Eileen Gentry, Professor and Head of the School of International Relations, University of St Andrews, Scotland, suggests amending just war theory by incorporating and considering the perspectives of NSAs.[27] Gentry argues that there is a bias against NSAs, which discounts their legitimate use of authority.[28] Conversely, there is a bias in favor of state

(Master Thesis, Leiden University); Vikrant Deshpande & Shibani Mehta, *Contextualising Hybrid Warfare*, *in* HYBRID WARFARE: THE CHANGING CHARACTER OF CONFLICT 26–28 (2018).

[22] Kevin D. Scott, *Joint Operating Environment 2015: The Joint Force in a Contested and Disordered World,* 2035 Joint Operating Env't 1, 6 (2016), http://fas.org/man/eprint/joe2035.pdf [https://perma.cc/VU94-LXZA]. *See also*, ZDZISŁAW ŚLIWA ET AL., *Russian Ambitions and Hybrid Modes of Warfare*, 7 SÕJATEADLANE EST. J. OF MIL. STUD. 95–98 (2018) (Est.); North Atlantic Treaty Org. (NATO) Legal Gazette, *Articles on NATO Current Challenges*, at 8–17, 37 (October 2016), http://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_37a.pdf [https://perma.cc/8F96-3Y89]; NADEEM ASHRAF, THE PURSUIT OF HYBRID WARFARE: MUDDLING TOWARDS CLARITY AND IMPLEMENTATION 7–8 (US Army War Coll., 2017), http://publications.armywarcollege.edu/pubs/3384.pdf [https://perma.cc/U9GU-LS4P]; European Commission Press Release IP/16/1227, Security: EU Strengthens Response to Hybrid Threats (Apr. 6, 2016).

[23] *See* Dubik, *supra* note 14, at 9–11.

[24] *See id.* at 25–26.

[25] *See* How We Fight, *supra* note 10. *See also* Pollard, *supra* note 10, at 93; Fisher, *supra* note 10, at 79.

[26] *See* Dubik, *supra* note 14, at 20–22.

[27] CARON E. GENTRY, *Epistemic Bias: Legitimate Violence & Politically Violent Non-State Actors*, *in* THE FUTURE OF JUST WARS: NEW CRITICAL ESSAYS (Caron E. Gentry & Amy E. Eckert, eds. 2014).

[28] *Id.*

actors who similarly use their authority.[29] This bias leads to all state actions being labelled legitimate and all activities of violent NSAs being labelled as illegitimate terrorism.[30] This Article explores, within the bounds of the future of just war theory, whether "legitimate authority" should be granted to NSAs. If this authority is granted, what are the possible pitfalls to sanctioning such authority? And if it should not be considered, then how is this epistemic bias adversely affecting the interests of NSAs?

This Article seeks to explore whether just war theory will continue to evolve, as it has over the centuries. The Article discusses the future of the concept of legitimate authority in jus ad bellum and the future of information warfare, while considering whether cyberattacks can be considered as the use of force. This Article also considers the underlying pivotal tactics of aggressive modern warfare within the realms of just war theory so that the practicality of the proposed amendments in just war theory, as expounded by Gentry, are better understood. If these proposals for changes in just war theory are compared to modern warfare tactics, the practicality of these proposals can be perceived in a more nuanced manner. Modern aggressive warfare techniques rely heavily on indirect warring tactics in fourth-generation, fifth-generation, and hybrid warfare, all of which involve routinely employing NSAs.[31] Therefore, it is in the interest of the states to exploit just war theory for their own interests.

For these reasons, this Article explores the tenets of bestowing legitimate authority upon NSAs to use force, while considering modern warfare tactics in accordance with the established norms in just war theory. Together, these tenets and the modern warfare tactics together provide the foundation for what the future of just war theory can and should look like.

This Article is divided into three Parts. Part I introduces and defines what just war theory is and briefly explicates its major tenets. Part I.A. deals with jus ad bellum and explains the notions of just cause, lawful

---

[29] *Id.*

[30] *Id.* at 24-26.

[31] *See The Four Generations of Modern War*, *supra* note 18. *See also*, *Understanding Fourth Generation Warfare*, *supra* note 18;*4GW: Our Enemies Play to Their Strengths*, *supra* note 18; The Sling and the Stone, *supra* note 18; Hammes's Insurgency, *supra* note 18; 4GW is Here!, *supra* note 18; Albert A. Nofi, *supra* note 18; Dreaming Fifth Generation War, *supra* note 19; Herring, *supra* note 19; Safranski, *supra* note 19; Weeks, *supra* note 19; Burke, *supra* note 19; Cyber Operations, *supra* note 20; Kaplan, *supra* note 20; Dinniss, *supra* note 20; Tallinn Manual, *supra* note 20; Guardian article, *supra* note 20; Cyber Terrorism, *supra* note 20; Toure, *supra* note 20.

authority, macro-proportionality, right intention, and last resort. It is followed by Part I.B, which describes jus in bello and briefly introduces the principles of proportionality, distinction, and military necessity. Part I.C explores the implications of jus post bellum. Thereafter, Part II discusses the future of information warfare and cyberwarfare within the context of just cause and considers the possibility of cyberattacks being considered an armed attack or a use of force, as required under Articles 2(4) and 51 of the UN Charter. Finally, Part III examines Gentry's argument for giving NSAs legitimate authority.[32]

I. JUST WAR THEORY

Just war theory emanated from Christian theologians and canonists and later became customary international law.[33] Just war theory evaluates the morality of wars, in contrast with realism, which excludes morality from its judgments.[34]

A. JUS AD BELLUM

Jus ad bellum involves prerequisites for waging a justified war. It includes the steps needed to justify the use of force against a target.[35] Jus ad bellum has five major requirements: (1) just cause, (2) legitimate authority, (3) right intention, (4) proportionality, and (5) last resort.[36] The UN Charter developed a bifurcated approach towards war. While the Charter prohibits the use and threat of force,[37] it provides an exception allowing the use of force in self-defense[38] and in cases where the United Nations Security Council (UNSC) authorizes such force.[39] However, because of the exclusive veto powers of the permanent five members of

---

[32] *See* GENTRY, *supra* note 27.

[33] John F. Coverdale, *An Introduction to the Just War Tradition,* 16 PACE INT'L L. REV. 221, 223 (Fall 2004).

[34] *Id.*

[35] BRIAN OREND, THE MORALITY OF WAR 67 (2013).

[36] Cao Qin, *The Classical Confucian Ideas of Jus ad bellum, in* COMPARATIVE JUST WAR THEORY: AN INTRODUCTION TO INTERNATIONAL PERSPECTIVES 157–58 (Luis Cordeiro-Rodrigues & Danny Singh eds., 2019). *See also* Brian Hallet, *Just War Criteria*, *in* 1 ENCYCLOPEDIA OF VIOLENCE, PEACE AND CONFLICT 257, 284–86 (Lester R. Kurtz & Jennifer Turpin eds., 1999).

[37] U.N. Charter art. 2(4).

[38] Ian Ralby, *Private Military Companies and the Jus ad bellum*, *in* THE OXFORD HANDBOOK OF THE USE OF FORCE IN INTERNATIONAL LAW 1131, 1144 (Marc Weller et al. eds., 2015).

[39] U.N. Charter arts. 39–42.

the UNSC, wars are rarely waged under this rule.[40] Spawned over centuries, the notion of jus ad bellum and the laws of war have developed significantly into their present form under the UN Charter. In doing so, the notion of jus ad bellum has become synonymous with *jus contra bellum* (the law against armed conflict itself).[41]

In classical times, just cause included actions undertaken to right a wrong,[42] such as fighting in defense, punishing an evil, or recovering what was wrongly taken.[43] The notions of "punishing an evil" and "righting a wrong" are no longer considered just cause to initiate a war.[44] In the nineteenth century, countries also fought over economic and territorial disputes.[45] This is not to say that those wars had no moral values or grounds in justice or the international legal system; rather, such issues did not carry enough weight to be justified as just causes to wage a full-fledged war.[46] Later, the horrors of World War I and II paved the way for restricting wars to only defensive purposes as a just cause[47] to maintain global peace and security.[48] World War I gave birth to the Kellogg-Briand Pact and the Covenant of the League of the Nations, under which states agreed to resolve all international disputes through peaceful means, without resorting to war.[49] And the violence of World War II gave rise to the UN Charter in 1949, which further developed the just causes of war by limiting them to only defensive purposes.[50]

Under positive international law, Article 2(4) of the UN Charter forbids all uses of force.[51] Article 2(4) states: "[A]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[52] Article 51

---

[40] WASEEM AHMAD QURESHI, THE USE OF FORCE IN INTERNATIONAL LAW 27 (2017) [hereinafter USE OF FORCE].

[41] *See* USE OF FORCE, *supra* note 40, at 28.

[42] ANTHONY F. LANG JR. ET AL., JUST WAR: AUTHORITY, TRADITION, AND PRACTICE 157–80 (2013).

[43] *See id.* at 171.

[44] *See* Coverdale, *supra* note 33, at 230–31.

[45] *Id.* at 230.

[46] *Id.*

[47] U.N. Charter arts. 2(4), 51.

[48] *Id.* arts. 39–42.

[49] *See* Coverdale, *supra* note 33, at 232.

[50] *Id.* at 230–34.

[51] U.N. Charter art. 2(4).

[52] *Id.*

of the UN Charter provides an exception to Article 2(4) in instances of armed attack in self-defense.[53] It states that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."[54]

Aside from self-defense, positive international law forbids all use of force, and a state can only resort to war in response to an armed attack.[55] Ever since positive international law introduced the prohibition on the use of force, states have relied on and manipulated customary international law (created by state practices and *opinio juris*) to invoke the analyses of jurists and scholars to suit their aggressive stances. Some states come up with new principles—devices of their own—to justify potentially illegitimate wars, allegedly in the name of humanitarian action, without UNSC authorization.[56] For instance, preemptive or anticipatory self-defense,[57] the responsibility to protect,[58] and the unwilling and unable test[59] are all concepts previously used to justify war in the name of humanitarian action.[60] However, under modern international war, all instances of war that do not involve an armed attack, self-defense, or UNSC authorization are prohibited.[61] As a result, although conducted under the guise of humanitarian efforts, these actions are not considered legitimate.

In classical times, just war theory aimed to remedy a wrong[62] and to punish evil.[63] Recently, modern just war theory has shifted toward self-defense as the only legitimate reason[64] for a state to resort to war.[65] The

---

[53] *Id.* art. 51.

[54] *Id.*

[55] *Id.* arts. 2(4), 51.

[56] *See supra* note 6.

[57] *See supra* note 7.

[58] Gagro, *supra* note 8; Chandler, *supra* note 8.

[59] Deeks, *supra* note 9; *Unwilling Test in Syrian Conflict*, *supra* note 9; *Reasonableness of Use of Force*, *supra* note 9.

[60] Deeks, *supra* note 9; *Unwilling Test in Syrian Conflict*, *supra* note 9; *Reasonableness of Use of Force*, *supra* note 9.

[61] U.N. Charter arts. 2(4), 39–42.

[62] *See* Lang, *supra* note 42.

[63] HAROLD PALMER, CHRISTIAN PACIFISM AND JUST WAR THEORY: DISCIPLESHIP AND THE ETHICS OF WAR, VIOLENCE AND THE USE OF FORCE 19 (2016).

[64] U.N. Charter arts. 2(4), 51.

[65] *See* Coverdale, *supra* note 33, at 230–34.

focus of just war theory has shifted from enacting justice to stopping aggression and maintaining global peace and security.[66] There are several reasons for this shift. First, the motivation for bringing change in just war theory was a response to the World Wars and the destruction possible in modern warfare.[67] Second, allowing states to resort to wars for exceptional reasons contradicted the absolute prohibition on wars.[68] Third, the shift developed in order to foster, develop, and maintain a super-sovereign authority (the UN) as a peacekeeper that would resolve all international disputes.[69]

In classical just war theory, the legitimate authority to declare war belonged to the supreme authority—that is, the heads of state—and only sovereign states had such authority. In St. Augustine's words, "the power to declare and counsel war should be in the hands of those who hold the supreme authority."[70] Other scholars, including James Turner Johnson, believe that such authority must reflect the defense of a state's people and the defense of international peace and security. He states that:

> [T]he state's right to war derives not from its de facto or 'coercive' sovereignty . . . but from its membership of an international community to the common good of which the state is ordered and to the law of which it is subject [an] act of war must retain a public and legal character. . . . When states employ force in defence of their particular interests they are justified in so doing only to the extent that, at the same time, their actions can be convincingly construed as a defence of the international order and a securing of the international common good.[71]

The goal of limiting the legitimate authority to declare war to sovereign states was to restrict warfare and to hold states accountable for their actions,[72] as otherwise it would be difficult for regulatory authorities to hold people accountable for violations of international humanitarian

---

66 *Id.* at 231-34.

67 *Id.* at 234–35.

68 *Id.* at 235.

69 *Id.* at 234–35.

70 ST. THOMAS AQUINAS, SUMMA THEOLOGICA, VOLUME III - PART II, SECOND SECTION 1354 (Fathers of the English Dominican Province, trans., Cosimo, Inc. 2007) (1911). *See also* Coverdale, *supra* note 33, at 248.

71 Coverdale, *supra* note 33, at 249.

72 Paul Rexton Kan, *Globalisation and the Just War Tradition: The Vexing Problem of Legitimate Authority, in* WAR AND VIRTUAL WAR: THE CHALLENGES TO COMMUNITIES 51, 52 (Rodopi 2004).

law,[73] a problem known as the principal-agent conundrum.[74] For instance, if NSAs are allowed to take up arms and wage wars on other states without the authorization of their host states or governments, accountability will be impeded[75] because it will become difficult to determine who is to be held responsible; this in turn could hinder the preservation of global peace and security. If, for argument's sake, NSAs are given legitimate authority to wage wars, aggressive states could easily exploit this loophole in the legal system by employing NSAs in proxy wars to avoid retribution and attribution themselves.[76] In modern warfare, even from a realist point of view, where NSAs have no legitimate authority, states routinely use NSAs such as mercenaries, rebel groups, and terrorists to wage proxy wars against targeted states, to destabilize regions, to change regimes,[77] and to suit states' illicit national interests.[78]

The discussion of granting legitimate authority to NSAs to use force applies to international armed conflicts, but what about internal civil wars? Do NSAs have legitimate authority to wage wars for their interests? Do NSAs have legitimate authority to use force? NSAs' use of force should only be considered legitimate in limited circumstances in domestic law, such as in instances of colonized states (e.g., states such as Palestine that have been wronged and oppressed by other states).[79] In addition to

---

[73] *See* KATERI CARMOLA, PRIVATE SECURITY CONTRACTORS AND NEW WARS: RISK, LAW, AND ETHICS 138 (Routledge 2010).

[74] *Id.*

[75] *See* CARMOLA, *supra* note 73, at 138.

[76] KEVIN D. SCOTT, JOINT OPERATING ENVIRONMENT 2035: THE JOINT FORCE IN A CONTESTED AND DISORDERED WORLD 6 (2016), https://fas.org/man/eprint/joe2035.pdf [https://perma.cc/5KCY-BJ8T]; Zdzisław Śliwa, Viljar Veebel & Maxime Lebrun, *Russian Ambitions and Hybrid Modes of Warfare*, 7 SÕJATEADLANE [EST. J. OF MIL. STUD.] 86, 96 (2018), https://www.baltdefcol.org/files/files/publications/HybridModes.pdf [https://perma.cc/9QD7-LGFS]; Andrés B. Muñoz Mosquera & Sascha Dov Bachmann, *Understanding Lawfare in a Hybrid Warfare Context*, NATO LEGAL GAZETTE, Oct. 2016, at 12–14, https://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_37a.pdf [https://perma.cc/4BW4-28P5]; NADEEM ASHRAF, THE PURSUIT OF HYBRID WARFARE: MUDDLING TOWARDS CLARITY AND IMPLEMENTATION 7 (U.S. Army War Coll., 2017), https://publications.armywarcollege.edu/pubs/3384.pdf [https://perma.cc/SAN2-PTGA]; European Commission Press Release IP/16/1227, Security: EU Strengthens Response to Hybrid Threats (Apr. 6, 2016), https://ec.europa.eu/commission/presscorner/detail/en/IP_16_1227 [https://perma.cc/4PWN-WGVN].

[77] *See* Robert SCHÜTTE, CIVILIAN PROTECTION IN ARMED CONFLICTS: EVOLUTION, CHALLENGES AND IMPLEMENTATION 183 (Springer Fachmedien Wiesbaden 2015).

[78] *See* Waseem Ahmad Qureshi, *Applying the Principle of Proportionality to the War on Terror*, 22 RICH. PUB. INT. L. REV. 379, 396–97 (2019) (hereinafter *Proportionality Principle War on Terror*).

[79] *See* Coverdale, *supra* note 33, at 238.

curtailing diffused responsibility,[80] restricting legitimate authority to states only—referred to as the state's monopoly on the use of force[81]—also helps to maintain states' internal status quo as well as the interstate status quo in international relations.

Dr. Joseph H. Campos argues that affording NSAs, such as terrorists, the legitimate authority to employ violence would effectively legitimize terrorism. Thus, national security discourse on legitimate authority of using force that distinguishes legitimate and illegitimate violence for NSAs is a "vehicle of moral and legal tour de force against terrorism."[82] Yet, there are advocates of NSAs who support the view that NSAs should have legitimate authority to wage war in the future.[83] This is understandable; aggressive states employ NSAs as pawns in their proxy wars as asymmetric tactics.[84] The utility that NSAs provide to states is high because using NSAs allows a state to avoid attribution and retribution,[85] and NSAs are cheaper to maintain than states' conventional armed forces.[86] Furthermore, NSAs are sometimes used by states because NSAs sometimes employ more efficient methods,[87] mainly because NSAs often do not adhere to the international humanitarian laws which protect the innocent during armed conflicts.[88] In contrast, conventional armed forces are required to adhere to humanitarian laws, because they and their states can be held accountable for their actions on the battlefield.[89] However, it is difficult if not impossible to hold NSAs accountable, practically speaking, since many NSAs do not have permanent locations or channels of communication. Furthermore, NSAs, by definition, do not belong to any

---

[80] CHRISTOPHER COKER, HUMANE WARFARE 65 (2001); CARMOLA, *supra* note 73, at 138.

[81] Anne Schwekenbecher, *Rethinking Legitimate Authority*, *in* ROULEDGE HANDBOOK OF ETHICS AND WAR 161. (Fritz Allhoff et al. eds., Routledge 2013).

[82] JOSEPH H. CAMPOS, THE STATE AND TERRORISM: NATIONAL SECURITY AND THE MOBILIZATION OF POWER 91 (Ashgate Publ'g 2007).

[83] *See* Gentry, *supra* note 27, at 25.

[84] *See* SCOTT, *supra* note 76, at 6; Śliwa, Veebel & Lebrun, *supra* note 76, at 96; Mosquera & Bachmann, *supra* note 76, at 7, 9, 12; ASHRAF, *supra* note 76, at 7; European Commission Press Release IP/16/1227, *supra* note 76.

[85] *See* SCOTT, *supra* note 76, at 6; Śliwa, Veebel & Lebrun, *supra* note 76, at 96; Mosquera & Bachmann, *supra* note 76, at 10, 12; ASHRAF, *supra* note 76, at 7. European Commission Press Release IP/16/1227, *supra* note 76.

[86] SEAN MCFATE, THE NEW RULES OF WAR: VICTORY IN THE AGE OF DURABLE DISORDER 130–31 (HarperCollins Publishers 2019).

[87] Fritz Alhoff, *The War on Terror and the Ethics of Exceptionalism*, *in* ROUTLEDGE HANDBOOK OF ETHICS AND WAR 203–210 (Fritz Allhoff, Nicholas G. Evans & Adam Heschke eds., 2013).

[88] *Id.*

[89] *Id.*

state, so no state can be held accountable on an NSA's behalf. NSAs sometimes deliberately target innocent civilians during armed conflicts to effectively harm a country.[90] An example of this practice is the Syrian war where NSAs, including rebels, mercenaries, and terrorists are being used on both sides of the conflict.[91]

In addition to requiring legitimate authority and just cause, under just war theory, a just war must be proportional and undertaken as a last resort.[92] In order for a war to be proportional under jus ad bellum, the benefits achieved must be proportional to their costs.[93] The destruction caused by a war cannot exceed the gains it achieves. Relatedly, the notion of "right intention" means that war must be waged for a justified cause and must not be waged for unjustified reasons.[94] Similarly, a war must have been used as a last resort in order for it to be justified.[95] This means that, before resorting to taking up arms and using force, all diplomatic and peaceful resources must be exhausted.[96] As an illustration of the last resort requirement, if State A undertakes surgical strikes at terrorists hiding in State B's territory, though State B can respond in proportionate manner, it cannot wage a full-fledged war in response without exhausting peaceful negotiations to end the conflict. These negotiations can explore ways to jointly investigate. Requiring war be a last resort allows peace to be restored without violence, and additionally keeps states' sovereignty intact. Nevertheless, if State A attacks State B without any justified cause, and State B exhausts all peaceful resources to end the conflict, it can wage a defensive war in response to defend its sovereignty.

However, the responsive attack, too, must be proportional to the extent of the threats posed by the initial armed attacks. It may be

---

[90] *Id.*

[91] *President Assad Accuses US of "Destabilising" Syria*, BBC, (July 8, 2012), https://www.bbc.com/news/world-middle-east-18763672 [https://perma.cc/CJ6G-JUNS]. *See also,* Mara Kramlin, *After 7 Years of War, Assad Has Won in Syria. What's Next for Washington?,* BROOKINGS, (Feb. 13, 2018), https://www.brookings.edu/blog/order-from-chaos/2018/02/13/after-7-years-of-war-assad-has-won-in-syria-whats-next-for-washington [https://perma.cc/764L-KGGN]; Mallory Shelbourne, *Study Shows US Weapons Given to Syrian Rebels Ended Up in ISIS Hands*, THE HILL, (Jan. 20, 2020). https://thehill.com/policy/defense/364917-study-shows-us-weapons-given-to-syrian-rebels-ended-up-in-isiss-hands [https://perma.cc/EAK2-DQ29].

[92] Qin, *supra* note 36, at 158. *See also* Hallet, *supra* note 36, at 258.

[93] *See* Coverdale, *supra* note 33, at 255.

[94] ANNE SCWENKENBECHER, TERRORISM: A PHILOSOPHICAL ENQUIRY 84–86 (2012).

[95] *Id.* at 101–04.

[96] *Id.*

impossible to exhaust all alternatives before resorting to the use of force.[97] Therefore, the last resort requirement does not mean that truly all alternatives must be exhausted. Instead, it means that war must be a least preferred option[98] as a response to a conflict.

B. JUS IN BELLO

Jus in bello is a component of just war theory, which is also referred to as international humanitarian law (IHL). Jus in bello regulates the conduct of parties taking part in an armed conflict.[99] It seeks to minimize the suffering of victims of armed conflicts during wars and the use of armed force.[100] Jus in bello consists of three principles established purely for humanitarian purposes: proportionality, distinction, and military necessity.[101]

There are two different ways in which the notion of proportionality is applied under the just war theory. In jus ad bellum, proportionality limits the power of a state to resort to force, while in jus in bello, it determines the means and magnitude of the use of force.[102] The International Committee of the Red Cross (ICRC), in explaining the principle of proportionality, states that "[l]aunching an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited."[103] The principle of proportionality is intended to restrict excessive violence and maintains that violence should only be used when necessary. Armed attacks are judged "in relation to the concrete

---

[97] J. DARYL CHARLES & TIMOTHY J. DEMY, WAR, PEACE, AND CHRISTIANITY: QUESTIONS AND ANSWERS FROM A JUST-WAR PERSPECTIVE 175 (2010).

[98] *See* Coverdale, *supra* note 33, at 259.

[99] *What are jus ad bellum and jus in bello?* ICRC, (Jan. 22, 2015), https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0 [https://perma.cc/QLE4-N8K5].

[100] *Id.*

[101] Mark Maxwell, *The Innocent Combatant: Preserving Their Jus in Bello Protections,* 5 PENN ST. J. L. & INT'L AFF. 111 (2017).

[102] Enzo Cannizzaro, *Contextualizing proportionality: jus ad bellum and jus in bello in the Lebanese war*, 88 INT. REV. RED CROSS 781 (Dec. 2006).

[103] Rule 14: Proportionality in Attack, Customary International Humanitarian Law, ICRC, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule14 [https://perma.cc/HJH6-GD4Z].

and direct overall military advantage anticipated."[104] The principle of proportionality is part of customary international law[105] and was adopted by Additional Protocol 1 to the Geneva Conventions (AP1).[106]

The principle of distinction protects civilian property and lives during armed conflict by labeling them as illegitimate targets and by providing a distinction between combatants and noncombatants. In defining the distinction, the ICRC stated that "[t]he parties to the conflict must at all times distinguish between civilians and combatants. Attacks may only be directed against combatants. Attacks must not be directed against civilians."[107] However, a civilian's shield from attack disappears when he or she chooses to take part in armed conflict or war. Similar to the principle of proportionality, the principle of distinction is part of customary international law,[108] and is substantiated by AP1.[109] The International Court of Justice (ICJ) has established that this principle is the basis of all humanitarian law, and it is indispensable in all situations during armed conflicts under customary international law.[110]

C. JUS POST BELLUM

Jus post bellum deals with the aftereffects of war, that is, what to do when a war ends.[111] It is a relatively new concept and is not part of classical just war theory. However, this concept is gaining traction, and will likely become a crucial part of just war theory in the future.[112] St.

---

[104] Rome Statute of the International Criminal Court, art. 8(2)(b)(iv), July 1, 2002, 2187 U.N.T.S. 38544.

[105] Rule 14: Proportionality in Attack, Customary International Humanitarian Law, *supra* note 103.

[106] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 51, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

[107] Rule 1: The Principal Distinction Between Civilians and Combatants, Customary International Humanitarian Law, ICRC, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule1 [https://perma.cc/7RD4-4Z3N].

[108] *Id.*

[109] Additional Protocol I, *supra* note 106, arts. 48, 51, ¶ 2, 52, ¶ 2.

[110] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ ¶ 78–79 (July 8).

[111] *See* Inger Osterdahl, *The Gentle Modernizer in the Law of Armed Conflict*, *in* JUS POST BELLUM: MAPPING THE NORMATIVE FOUNDATIONS 224 (Carsten Stahn, Jennifer S. Easterday & Jens Iverson eds., 2014) (discussing the background and recent developments in *jus post bellum* theory and its potential effect on the law of armed conflict).

[112] *See* Albert W. Klein, *Attaining Post-Conflict Peace Using the jus post bellum Concept*, 11 Religions, Apr. 8, 2020, https://doi.org/10.3390/rel11040173 [https://perma.cc/J9K5-N45P].

Augustine believed that "it is an established fact that peace is the desired end of war. For every man is in quest of peace, even in waging war, whereas no one is in quest of war when making peace."[113] John Rawls, an American political philosopher, wrote that once peace is securely re-established, the enemy society is to be granted an autonomous well-ordered regime of its own. (For a time, however, limits may be rightly placed on the defeated society's freedom in foreign policy.) This means that enemy civilians are not to be held as slaves or serfs after surrender or denied their full liberties indefinitely.[114] This shows that scholars have been considering jus post bellum for a long time.

Once a war is over, the sovereignty of a defeated state should be restored as soon as is feasible. The victor should not have any right to control the conquered territories, to rule it by installing a puppet government, or to colonize it.[115] In modern warfare, the aggressors, even in legitimate wars, may plunder all the natural resources of the defeated.[116] Similarly, there have been cases where all the gold in the national reserve of the defeated country is pillaged by the victors,[117] just as it used to be in the Dark Ages. Thus, in future articulations of just war theory, the law must protect the sovereignty and resources of a defeated country. Otherwise, some states, with or without just causes of war, may continue to enrich themselves by preying on the weak.

To conclude, under the present standard articulation of just war theory, the use of force in self-defense and under UNSC authorization are the only justified reasons to go to war,[118] and only states have the legitimate authority to decide to use force and declare war.[119] Moreover, to restrict violence and to safeguard the peace and security of this world, the use of force must be the last resort after exhausting all feasible peaceful solutions.[120] This legal framework of international law intends to foster peace. This reasoning is also bolstered by the fact that humanitarian laws

---

[113] Gary J. Bass, *Jus Post Bellum*, 32 PHIL. & PUB. AFF. 384, 387 (2004) (quoting ST. AUGUSTINE, CONCERNING THE CITY OF GOD AGAINST THE PAGANS 866 (Henry Bettenson trans., Penguin Books 1984)).

[114] *Id.* at 388 (quoting JOHN RAWLS, THE LAW OF PEOPLES 98 (Harvard University Press 1999)).

[115] *Id.*

[116] *See, e.g.,* UGO MATTEI & LAURA NADER, PLUNDER: WHEN THE RULE OF LAW IS ILLEGAL 118-19 (2008).

[117] *See, e.g.,* RICHARD A. SCHWARTZ, ENCYCLOPEDIA OF THE PERSIAN GULF WAR 92 (2015).

[118] U.N. Charter art. 2, ¶ 4, arts. 39–51.

[119] PAUL R. KAN, WAR AND VIRTUAL WAR: THE CHALLENGES TO COMMUNITIES 52 (2004).

[120] SCHWENKENBECHER, *supra* note 94, at 101.

under jus in bello have also protected innocent lives during armed conflicts.[121] However, in employing modern warfare tactics, states constantly formulate new means to justify their aggression while at the same time avoiding attribution and retribution for armed attacks.[122] Information warfare, as well as the employment of NSAs as proxy warriors in current times, are some examples of such tactics that evade the existing framework of just war theory. Therefore, it is pertinent to explore whether just war theory can inform the question of how to deal with the threat to peace created by information warfare and the use of NSAs.

II. INFORMATION WARFARE

Just war theory and laws regarding the use of force guide the use of armed attacks.[123] But modern warfare techniques use tools such as cyberwarfare and informational tools to attack other states without a direct armed attack. These attacks are capable of inflicting damages equivalent to the destruction caused by kinetic warfare.[124] This raises the questions of whether cyberattacks can be considered a form of aggression that may be addressed by just war theory, and also whether future iterations of just war theory can even incorporate new forms of modern warfare such as cyberattacks.

Information warfare is defined as "actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary."[125] This definition was deliberately drafted to be broad so as to include the continuously evolving relationship between information and conflicts.[126] Under this definition, hacking a computer that is located in the

---

[121] *See* Additional Protocol I, *supra* note 106. *See also* Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 75 U.N.T.S. 287 [hereinafter *Geneva Convention IV*].

[122] Scott, *supra* note 22. *See also* Śliwa, *supra* note 22, at 96; Baillat, *supra* note 22; Ashraf, *supra* note 22, at 7–8; Press Release, *supra* note 22.

[123] U.N. Charter arts. 2, ¶ 4, 39–51.

[124] For example, the Stuxnet virus attack on Iran by the U.S. and Israel destroyed hundreds of centrifuges in Iranian nuclear refinement facilities. *See* DAVID SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER (Crown 2012).

[125] Michael W. Johnson, Just-War Theory and Future Warfare 70 (June 2, 1999) (unpublished MMAS thesis, U.S. Army Command and General Staff College), https://apps.dtic.mil/sti/pdfs/ADA383941.pdf (quoting DOROTHY E. DENNING, INFORMATION WARFARE AND SECURITY 10 (1990)) [https://perma.cc/PZE7-JBYU].

[126] *Id.*

territory of another state is considered information warfare, as is dropping "2,000 bombs" on the telecommunication networks of another county.[127]

Information warfare can be classified into two categories based on its intensity: higher-intensity information warfare, also known as cyberwarfare, and low-intensity information warfare, which is classified as netwar.[128] Cyberwarfare has been described as "conducting and preparing to conduct military operations according to information principles,"[129] and netwar has been described as "societal-level conflict waged through inter-netted modes of communication."[130] In both netwar and cyberwarfare, NSAs are used as "ethno-nationalists, separatists, criminal organizations, commercial predators, militant NGOs, revolutionary movements, militia, smugglers, and terrorists."[131] This illustrates that information warfare is often waged using more modern ways of fighting wars, whereas NSAs or mercenaries are employed to further political or personal gains. By employing NSAs in modern warfare, the lines between peace and wartime, and between combatants and noncombatants, is conveniently blurred. Therefore, to combat these evolving warfare techniques, new strategies must be adopted in classical just war theory.[132]

Scholars predict that cyberwarfare will likely be a weapon of choice in the future[133] and that it will be a major national security issue in this century.[134] While hacking attacks may seem trivial and relatively harmless, scholars believe that denial-of-service attacks in the e-commerce sector, for example, an attack on Amazon's website, could alone create billions of dollars in damages.[135]

Cyberattacks come in numerous forms. Hackers that engage in cyberespionage, for example, steal confidential data or information in

---

[127] *Id.*

[128] *Id.* at 71 (citing JOHN ARQUILLA & DAVID RONFELDT, THE ADVENT OF NETWAR 3 (1996)).

[129] *Id.*

[130] *Id.*

[131] JOHN ARQUILLA & DAVID RONFELDT, THE ADVENT OF NETWAR 47–80 (1996).

[132] *See* Johnson, *supra* note 125, at 71.

[133] ARQUILLA & RONFELDT, *supra* note 131, at vii; JOHN ARQUILLA & DAVID RONFELDT, CYBERWAR IS COMING! 144–45 (1993).

[134] *See* Richard W. Aldrich, *The International Legal Implications of Information Warfare,* U.S. A.F. ACAD.:INST. FOR NAT'L SEC. STUDIES, 1–2 (Apr. 1996), http://www.iwar.org.uk/law/resources/iwlaw/aldrich.htm [https://perma.cc/X96D-FNUQ]; SENATE SELECT COMMITTEE ON INTELLIGENCE, ANN. THREAT ASSESSMENT 39 (Feb. 12, 2009).

[135] *See* Johnson, *supra* note 125, at 73.

cyberspace.[136] Examples of cyberespionage include Google's allegation that a group of NSAs hacked the email addresses of Chinese human rights activists[137] and Russia's allegation that the United States and Israel obtained sensitive information from Iranian oil companies.[138] The United States has also alleged that Chinese hackers downloaded confidential and sensitive data on F-35 fighter jets, which posed a national security threat.[139] Some leaked documents of the United States National Security Agency by NSAs also proved that heads of state were under surveillance by the United States government, an example of cyberespionage that threatened state sovereignty.[140]

Other than cyberespionage, cyberterrorism also has the potential to disturb global peace and security. For instance, in 2010, the United States and Israel used the Stuxnet virus to target Iranian nuclear facilities that destroyed numerous centrifuges.[141] Similarly, in 2007, Israel attacked the Iranian radar system with cyberwarfare technology in an attempt to weaken the Iranian defense system against Israeli attacks on Iranian nuclear facilities.[142]

According to the United Nations General Assembly (UNGA) Resolution 66/24 of 2011, "[s]overeignty and international norms and principles that flow from sovereignty apply to state conduct of ICT [information and communication technology]-related activities."[143] The UN Secretary-General substantiated this UNGA claim by arguing that "ICT security in the existing framework of international law and

---

[136] *See* MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 2, 3, 20 (2013).

[137] David Drummond, *A New Approach to China*, GOOGLE: OFFICIAL BLOG (Jan. 12, 2010), https://googleblog.blogspot.com/2010/01/new-approach-to-china.html [https://perma.cc/SE9A-YC4G].

[138] Ellen Nakashima et al., *U.S, Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say*, WASH. POST (June 19, 2012), https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html [https://perma.cc/89BT-YBLR].

[139] Alexander Melnitzky, *Defending America Against Chinese Cyber Espionage Through the Use of Active Defenses*, 20 CARDOZO J. INT'L & COMP. L. 537, 545 (2012).

[140] Russell Buchan, *Cyber Espionage and International Law*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBER SPACE 179 (Nicholas Tsagouris & Russell Buchan, eds., 2015).

[141] SANGER, *supra* note 124, at 188. Sanger describes a cyberattack carried out by the United States and Israel against Iran as beginning in 2007 and 2008, *id.* at 188–89, and widespread reporting naming the virus 'Stuxnet,' *id.* at 203–05. *See also* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 13 (Jens David Ohlin et al. eds., 2015).

[142] PETER W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 126–28 (2014).

[143] G.A. Res. 68/243, n. 4 (Dec. 27, 2013) (adopting a 2013 report *infra* note 144).

understandings that govern state relations [] provide the foundation for international peace and security."[144] Russell Buchan has said that the Article 2(4) prohibition on the use of force includes cyberespionage.[145] Similarly to Buchan, Melnitzky also argues that Article 2(4) of the UN Charter includes cyberespionage, because it threatens global peace and security.[146]

Arguably, cyberespionage and cyberattacks do come within the prohibition on the use of force and under the principle of noninterference.[147] For instance, in the Stuxnet attack of 2010, the United States and Israel did not meet the requisite criteria of just war theory when they attacked Iran, because an unprovoked attack on a UN member violates the prohibition on the use of force, as stated in Article 2(4) of the UN Charter.[148] This attack also pierced the political integrity and sovereignty of Iran. This application of just war theory in the cyberattack context is equally applicable to NSAs, as NSAs are also bound by the prohibition on the use of force and the principle of nonintervention in other states.

However, according to the legalist paradigm, nothing but armed attack by an aggressor can justify war.[149] Under this paradigm, can cyberattacks be considered an armed attack? What kind of recourse is available to victim states for cyberattacks under just war theory? Since cyberattacks typically do not cause deaths or shock the moral conscience, Walzer has argued that it is still debatable whether cyberattacks are sufficient to justify war or even armed attacks in response.[150] If the victim state chooses to use force in retaliation to cyberattacks by NSAs without exhausting amicable options, then the victim state cannot violate the sovereignty of the host state where NSAs are residing in accordance with the legalist paradigm.[151] If the cyberattack has merely caused damage to

---

[144] Foreword by U.N. Secretary-General, to Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, at 4, U.N. Doc. A/68/98 (June 24, 2013) [hereinafter Developments in Information and Telecommunications].

[145] *Id.* at 187.

[146] Melnitzky, *supra* note 139, at 553–54.

[147] Ella Shoshan, Applicability of International Law on Cyber Espionage Intrusions 2 (Autumn 2014) (unpublished law thesis, Stockholm Univ.), http://www.diva-portal.org/smash/get/diva2:799485/FULLTEXT01 [https://perma.cc/D3YY-BMSW].

[148] U.N. Charter art. 2, ¶ 2; *id.* arts. 39–51.

[149] *See* Johnson, *supra* note 125, at 76.

[150] *Id.*

[151] *Id.*

e-commerce or a similar intangible system, then these attacks would be the last resort.

But if the use of force in response to cyberattacks is considered unjust in just war theory, then what options does a victim state have to defend itself against cyberattacks by NSAs or by states that violated its sovereignty and political integrity? Because of the limited options available to victim states, cyberattacks by NSAs pose a lacuna in just war theory, which can be exploited by states to launch attacks on the targeted states. These clandestine means are often employed to avoid attribution or retribution for any attacks.[152] Consequently, in today's age of technology, it is difficult to identify the perpetrators of cyberattacks. These attacks can cause billions of dollars in damage and leave the victims unable to take any action because they cannot identify the perpetrators. Future just war theory must be expanded to include cyberattacks to right the wrongs of technological aggression.

A. CYBERATTACKS AS THE USE OF FORCE

As discussed earlier, a variety of attacks, be they through cyber means or information, can easily come under the definition of the principle of non-intervention, and can violate a state's political sovereignty. Can the attack be considered a use of force that justifies the responsive use of force in self-defense? If yes, then how can a kinetic use of force ever be proportional to any cyberattack and why? It is believed that, if the effects of information warfare or cyberattacks are such that they match the destruction of an armed attack, then the attacks can be considered a use of force in violation of Article 2(4),[153] giving rise to the right to use force in self-defense under the aegis of the UN Charter.[154] The Tallinn Manual on cyberwarfare says that "cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level

---

[152] Nicolò Bussolati, *The Rise of Non-State Actors in Cyberwarfare*, *in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 118 (Jens David Ohlin et al. eds., 2015).

[153] Marco Roscini, *Cyber Operations as a Use of Force, in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 233, 242 (Nicholas Tsagourias & Russell Buchan eds., 2015). *See also* Carlo Focarelli, *Self-Defense in Cyberspace*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 255, 267 (Nicholas Tsagourias & Russell Buchan eds., 2015).

[154] Roscini, *supra* note 153, at 242. *See also* Focarelli, *supra* note 153, at 266.

of a use of force."[155] Harold Koh, the former legal advisor of the State Department, has also suggested that cyberattacks can be considered a use of force "if the physical consequences of a cyber-attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber-attack should equally be considered a use of force."[156] Though the destruction caused by cyberattacks are not direct in effect,[157] the decision of the ICJ in the *Nicaragua* case substantiates this argument by stating that the use of force or armed attack can indeed be indirect in nature.[158] The 1982 United States cyberattack that destroyed a gas pipeline in the Soviet Union, and the Stuxnet attack of 2010 by Israel and the United States, are examples which demonstrate that cyberattacks can create destruction equivalent to conventional armed attacks[159] and thus should be considered to be a use of force.

The use of force in self-defense is only justified when it is undertaken in retaliation to an armed attack under Article 51 of the UN Charter.[160] One could argue that because cyberattacks are not armed attacks per se, states do not have a right to respond with defensive force. However, if the threshold of destruction caused by cyberattacks matches the effect of damage caused by conventional armed attacks, then it can give rise to the right to use defensive force in response to cyberattacks.[161] Consequently, if the aftermath of cyberattacks or armed attacks are the same, then it does not matter what means were employed to achieve such results. Article 2(4) of the UN Charter does not in itself provide any limits for such a threshold. Therefore, any attack that can be considered a use of force is arguably prohibited under the UN Charter.[162] For instance, in 2012, the United States attacked the largest oil company of Saudi Arabia

---

[155] MICHAEL SCHMITT, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO THE CYBER WARFARE 45 (2013).

[156] Applicability of International Law to Hostilities in Cyberspace, 2012 DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW, ch. 18, §A(1)(c), at 593–95 [hereinafter *Digest*]; Harold Koh, *International Law in Cyberspace*, HARV. INT'L L.J. 1, 4 (2012).

[157] *See* Roscini, *supra* note 153, at 242–43.

[158] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgement, 1986 I.C.J. 14, ¶ 205 (June 27). *See also* DINNISS, *supra* note 20, at 50.

[159] THOMAS RID, CYBER WAR WILL NOT TAKE PLACE 4 (2013). *See also,* DAVID ALBRIGHT ET AL., INST. FOR SCI. & INT'L SEC., DID STUXNET TABLE OUT 1,000 CENTRIFUGES AT THE NATANZ ENRICHMENT PLANT? 1–2 (2010); Roscini, *supra* note 153, at 243.

[160] *See* U.N. Charter art. 2, ¶ 4; *id.* art. 51.

[161] OLIVIER CORTEN, THE LAWS AGAINST WAR: THE PROHIBITION ON THE USE OF FORCE IN THE CONTEMPORARY INTERNATIONAL LAW 55, 66–67 (2010). *See also Digest*, *supra* note 157, at 595.

[162] *See* U.N. Charter art. 2, ¶ 4; *id.* art. 51.

with a computer virus which ultimately destroyed thirty thousand of its computers.[163] An attack of this size can be considered to have violated the prohibition on the use of force[164] as well as the principle of non-intervention[165] in a sovereign territory. Likewise, any cyberattacks on a country's defence system or other important infrastructure can also be considered a use of force against that country's sovereignty.[166] Countries including the United States,[167] Mali,[168] and Russia[169] already consider this kind of attack to be a use of force.

However, an opposing view is that cyberattacks are not armed attacks.[170] Proponents of this view posit that cyberattacks do not use conventional kinetic energy and should therefore only be considered political and economic coercion.[171] However, this view is flawed. In contrast, Roscini argues that political and economic coercion uses diplomatic, political, and economic means, whereas cyberattacks use

---

[163] *Saudi Aramco Says Cyber Attack Targeted Kingdom's Economy*, AL ARABIYA ENG. (U.A.E.) (Dec. 9, 2012), https://english.alarabiya.net/en/News/2012/12/09/Saudi-Aramco-says-cyber-attack-targeted-kingdoms-economy.html [https://perma.cc/TE2M-M5ZQ].

[164] *See* John F. Murphy, *Cyber War and International Law: Does the Intentional Legal Process Constitute a Threat to U.S. Vital Interests?*, 89 INT'L L. STUD. 309, 325 (2013).

[165] *See* Terry D. Gill, *Non-Intervention in the Cyber Context, in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBER-SPACE 217, 235 (Katharina Ziolkowski ed., 2013).

[166] *See, e.g., US Drones Infected by Key Logging Virus*, AL JAZEERA (Qatar) (Oct. 8, 2011), https://www.aljazeera.com/news/americas/2011/10/201110816388104988.html (describing effects of a virus on the US military's unmanned drones) [https://perma.cc/YB2H-6523]; Robert Johnson, *New Evidence Suggests China's Hacking into US Drones Using Adobe Reader and Internet Explorer*, BUS. INSIDER (Dec. 22, 2011), https://www.businessinsider.com/chinas-hacking-into-us-drones-using-adobe-reader-and-internet-explorer-2011-12 (reporting that China is likely behind viruses targeting US drones) [https://perma.cc/S3UV-EV74]; Charles Arthur, *Chinese Hackers Suspected of Interfering with US Satellites*, GUARDIAN (London) (Oct. 27, 2011), https://www.theguardian.com/technology/2011/oct/27/chinese-hacking-us-satellites-suspected (explaining how a foreign country's access to satellite controls could physically affect the satellite) [https://perma.cc/27HJ-HU3U].

[167] U.S. DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 15, 18 (1999); U.S. DEP'T OF DEF., CYBER SPACE POLICY REPORT, 9 (2011); CYBER OPERATIONS, *supra* note 20, at 6–8; U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 18–19, U.N. Doc. A/66/152 (July 15, 2011) (hereinafter *Developments in Information and Communications 2011*).

[168] U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 8, U.N. Doc. A/64/129/Add.1 (Sept.9, 2009).

[169] Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL L. REV. 132, n. 124 (2005) (quoting Steven A. Hildreth, *Cyberwarfare*, 13–14, CRS Report for Congress, RL30735 (June 19, 2001)).

[170] Elizabeth Wilmshurst, *The Chatham House Principles of International Law on the Use of Force in Self-Defence*, 55 INT'L & COMP. L.Q. 963, 965 (2006).

[171] *See id.*

cyber means to destroy targets. Roscini adds that it should not matter what kind of energy—kinetic or not—is used to destroy a target; if the outcome is similar to that which would result from the use of conventional weapons, then it is an armed attack.[172] In the past, international law has considered the "arming and training of groups,"[173] the illegal use of force, sanctioning a naval blockade, provisioning of lands to an aggressor, and even breaching a treaty to be considered the use of force.[174] Altogether, the law is flexible enough to allow for the ever-changing tactics of war, because the goal of the law in the first place was to prohibit intervention and aggression toward victim states.[175] Therefore, cyberattacks–unlike economic and political coercions–can be considered armed attacks if the destruction caused is equivalent to that of kinetic energy weapons.[176]

The UN Charter was drafted long before the age of the internet. Therefore, the drafters could not have anticipated cyberattacks. Similarly, the UN Charter also does not include many other actions that could be considered to be use of force. Not all forms of coercion or uses of force will be cataloged somewhere. Alternatively, we must simply analyze the outcome of an attack to determine whether it can be considered a use of force. Therefore, cyberattacks meeting the same threshold as conventional armed attacks or uses of force can be considered to be prohibited under the UN Charter.[177]

In considering the *opinio juris* on the categorization of cyberattacks as the use of force or armed attacks, many countries[178]

---

[172] *See* Roscini, *supra* note 153, at 249.

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

[174] G.A. Res. 3314 (XXIX), art. 3 (Dec. 14, 1974).

[175] *See* DINNISS, *supra* note 20, at 45.

[176] *See* Roscini, *supra* note 153, at 249.

[177] Erik M. Mudrinich, *Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, 68 AIR FORCE L. REV. 167, 191 (2012). *See also* Roscini, *supra* note 153.

[178] János Martonyi, Minister of Foreign Affairs of Hungary, Speech at the Budapest Conference on Cyberspace (Oct. 4, 2012) (*transcript available at* https://2010-2014.kormany.hu/en/ministry-of-foreign-affairs/speeches-publications-and-interviews/minister-of-foreign-affairs-janos-martony-s-speech-at-the-budapest-conference-on-cyberspace [https://perma.cc/ZU2U-DPDU]); U.N. Secretary-General, *Developments in the Field of Information and Communications in the Context of International Security*, 3, U.N. Doc A/57/166/Add. 1 (Aug. 29, 2002) (describing Cuba's position); Alireza Miryousefi & Hossein Gharibi, *View from Iran: World Needs Rules on Cyberattacks*, CHRISTIAN SCIENCE MONITOR (Feb. 14, 2013), https://www.csmonitor.com/Commentary/Opinion/2013/0214/View-from-Iran-World-needs-rules-on-cyberattacks (explaining Iran's view that cyberattacks may be a use of force under Article 2(4)) [https://perma.cc/GK8U-DV3K]; U.N. Secretary-General, *Developments in the Field of*

including China,[179] Australia,[180] the UK,[181] and the United States[182] consider cyberattacks to be armed attacks or the use of force, and that the prohibition of the use of force means prohibition on cyberattacks within the meaning of Article 2(4) of the UN Charter. Russia has also noted that

> [F]rom a military point of view, the use of information warfare means against Russia or its armed forces will categorically not be considered a non-military phase or its armed forces will categorically not be considered a non-military phase of a conflict, whether there were casualties or not. . . . Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself.[183]

On the other hand, many states including China,[184] India, the UK, the United States, France, New Zealand, Germany, and Canada have been victims of cyberattacks, but the majority have chosen not to respond by the use of retaliatory force because they see cyberattacks as the equivalent of cyberespionage.[185] This is primarily because the international community is reluctant to define a cyberattack as a conventional use of force, because, with one exception, none of the cyberattacks have caused death or even injury to human beings.[186] One can sympathize with the view that where the retaliatory use of force in response to cyberattacks causes human injury or human deaths, it is disproportionate to the initial force used. However, this does not preclude cyberattacks from being considered a use of force. It follows that proportional retaliatory attacks are

---

Information and Communications in the Context of International Security, 7, U.N. Doc A/64/129/Add. 1 (Sep. 9, 2009); *Cybersecurity Strategy of European Union: An Open, Safe and Secure Cyberspace*, at 15–16, COM (2013) 1 final (Feb. 7, 2013); HR Doc. 33000-X No. 79 (2012), at 5–6 (Neth.); U.N. Secretary-General, *Developments in the Field of Information and Communications in the Context of International Security*, 9-10, U.N. Doc A/65/154 (Jul. 20, 2010).

[179] Li Zhang, *A Chinese Perspective on Cyber War*, 94 INT'L REV. RED CROSS 801, 804 (2012).

[180] *Developments in Information and Communications 2011*, *supra* note 168, at 6.

[181] *Id.*

[182] *See* Roscini, *supra* note 153, at 234.

[183] *See* DINNISS, *supra* note 20, at 54.

[184] John Leyden, *France Blames China for Hack Attacks*, REGISTER (UK), (Sept. 12, 2007). https://www.theregister.com/2007/09/12/french_cyberattacks/ [https://perma.cc/4VZC-8Y3G]. *See also* Edward Cody, *Chinese Official Accuses Nations of Hacking*, WASH. POST (Sept. 13, 2007), https://www.washingtonpost.com/wp-dyn/content/article/2007/09/12/AR2007091200791.html [https://perma.cc/8Q5W-NGUZ]; KREKAL ET AL., NORTHROP GRUMMAN, COMPATIBILITY OF THE PEOPLE'S REPUBLIC OF CHINA TO CONDUCT CYBER WARFARE AND COMPUTER NETWORK EXPLOITATION PREPARED FOR THE US-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION 19, 21–22 (2009).

[185] *See* DINNISS, *supra* note 20, at 55.

[186] *Id.* at 57.

permissible in self-defense. Therefore, if Iran's nuclear facilities are attacked (as they were in 2010 by the Stuxnet virus), Iran should have the right to use defensive cyber force against Israel and the United States as retribution. But what about situations where the victim state has no cyber technological capabilities to conduct such a defensive attack? What if Iran lacks the technological capacity or means to attack American or Israeli nuclear plants in response to the cyberattack on the Iranian nuclear facilities? For this reason, it is still debatable whether the conventional use of force in response to cyberattacks is justified or permitted under international law.

Based on these arguments and the *opinio juris* of the UN members, the UNGA report of 2013 concluded that cyberattacks can be considered a use of force. The report said that "international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment."[187] The report sets three conditions for cyberattacks for this purpose. The first condition dictates that the cyberattacks must be attributable to a state. The second condition requires that the effect of the cyberattack be equivalent to the conventional use of force, such as causing destruction of life or property. The third condition states that a cyberattack must be international in nature, violating the sovereignty of a state.[188] This incorporation of cyber warfare in the realm of just war theory shows that the legal framework of using force is flexible enough to cater to modern emerging warring tactics. The UNGA conditions do not obstinately require that only the conventional weapons are capable of inflicting destruction. Instead, the conditions are malleable and receptive to incorporating unconventional weapons or modern tools that are capable of destruction equivalent to that of conventional weapons.

The UNGA stance solidifies the argument that kinetic energy is not the defining element to interpret prohibition on the use of force and the principle of non-intervention, and that the means employed to attack a state do not matter; as long as the result is equivalent to that of a conventional use of force, the attack will also be considered a use of force.[189] The UNGA report also substantiates the idea that cyberattacks

---

[187] Developments in Information and Telecommunications, *supra* note 144, at 8.

[188] *See* Roscini, *supra* note 153, at 234.

[189] *Id.*

can be considered a use of force and can give rise to the right to use defensive force if that cyberattack can be attributed to a particular state.[190]

III. GENTRY'S LEGITIMATE AUTHORITY

In the vast majority of cyberattacks, the attacking state seeks to avoid detection and attribution,[191] which in turn allows them to evade retribution. In the context of cyberwarfare and information warfare, the states that wage wars are similarly employing NSAs to avoid attribution and retribution.[192] However, the current legal framework does not allow using proxy non-state actors during warfare.[193] Therefore, for the convenience of avoiding attribution and retribution by the attacking states, scholars such as Gentry support the view that actions of NSA are legitimate. While assessing the future of just war theory, Gentry,[194] along with Virginia Held[195] and Tarik Kochi,[196] argue that there is an international bias toward the established notion of lending political and moral legitimacy of authority to states to wage wars.

For Gentry, this epistemic bias is premised on traditional notions of statehood, warcraft, and moral legitimacy in a Westphalian sense. Gentry believes that the classic conception of legitimate authority is biased because it marks all state acts as legitimate but categorizes all activities of violent NSAs as illegitimate.[197] Gentry believes that the moral and political aspects of the Westphalian construct, which consider NSAs to be outsiders in legitimate authority, are unjust. Since both classical and contemporary positions of just war theory include political and moral aspects of legitimate authority, proponents of endorsing legitimate authority for NSAs rely on these concepts.[198] The notion of legitimate

---

[190] *Id.*

[191] RID, *supra* note 159, at 158.

[192] Mark Klamberg, *Exploiting Legal Thresholds, Fault-lines and Gaps in the Context of Remote Warfare, in* RESEARCH HANDBOOK ON REMOTE WARFARE 186–89 (Jens David Ohlin ed., 2017).

[193] Additional Protocol I, *supra* note 106, art. 44, ¶ 7. *See also* Toni Pfanner, *Military Uniforms and the Law of War*, 86 INT'L REV. RED CROSS 93 (2004).

[194] *See* GENTRY, *supra* note 27.

[195] VIRGINIA HELD, HOW TERRORISM IS WRONG: MORALITY AND POLITICAL VIOLENCE (2008). *See also* GENTRY, *supra* note 27, at 25–26.

[196] TARIK KOCHI, THE OTHER'S WAR: RECOGNITION AND THE VIOLENCE OF ETHICS (2009). *See also* GENTRY, *supra* note 27, at 25–26.

[197] GENTRY, *supra* note 27; MIRANDA FRICKER, EPISTEMIC INJUSTICE: POWER AND THE ETHICS OF KNOWING (2007).

[198] *See* GENTRY, *supra* note 27, at 17.

authority goes back to Aristotle's and Plato's depictions of the entrustment of the common good to individuals or institutions,[199] coupled with the bifurcation of good and evil.[200] According to Gentry, the "good" here only protects the political interests, while deemphasizing the "bad," which are the trivial interests of smaller factions of a society.[201] Gentry argues that morality is the defining characteristic of legitimate authority, which only protects political affairs.[202] This may be theoretically true, but in a practical sense, morality is not limited to the political affairs of a state regarding legitimate authority, as it has more to do with the common good of a nation. If legitimate authority is conferred on NSAs, then waging war, even with legitimate authority, will violate all major principles of international laws of force.[203]

As per the basic principal-agent conundrum,[204] emboldening legitimate authority for NSAs will diffuse the responsibility of an attack. This indicates that without a clear hierarchy of government system and state military, there will be too many hands to be held accountable in relation to an armed attack conducted by NSAs. The advocates of approving legitimate authority for NSAs such as Caron Gentry and Miranda Fricker do not discuss the implications of many hands in diffused responsibility. Therefore, it is vital to discuss the notion of legitimate authority in relation to its endorsement of NSAs.

Gentry moderates her argument by delving into the historical development of legitimate authority and by downplaying the ethical conflation attached to the notion of sovereignty.[205] Legitimate authority can be defined as whatever authority happens to be in place within a state that can mobilize the state's armies.[206] For Gentry, legitimacy is tied to the

---

[199] Henrick Syse & Helene Ingierd, *What Constitutes a Legitimate Authority?*, 24 SOC. ALTERNATIVES, no. 3, 2005, at 11, 12; GENTRY, *supra* note 27.

[200] Syse & Ingierd, *supra* note 199, at 12. *See also* GENTRY, *supra* note 27.

[201] GENTRY, *supra* note 27. *Accord* Syse & Ingierd, *supra* note 199, at 14.

[202] *See* GENTRY, *supra* note 27, at 17.

[203] *See, e.g.*, *Proportionality Principle War on Terror*, *supra* note 79, at 397; U.N. High Commissioner for Refugees, *International Protection Considerations with Regard to People Fleeing the Syrian Arab Republic Update V*, U.N. Doc. HCR/PC/SYR/17/01, 15–23 (Nov. 2017).

[204] *See* CARMOLA, *supra* note 73, at 138.

[205] GENTRY, *supra* note 27.

[206] James Turner Johnson, *Aquinas and Luther on War and Peace*, 31 J. RELIGIOUS ETHICS, Spring 2003, at 3, 7. *See also* GENTRY , *supra* note 27, at 18.

moral good for society.[207] Practically, however, legitimacy has to do more with law and less with morality. Legitimacy in authority, in fact, is when a governmental body

> [i]s entitled to have its decisions and rules accepted and followed by others. In the case of law, people feel a personal responsibility to comply voluntarily with those laws that are created and enforced by legitimate legal authorities. In contrast to morality, legitimacy is a general acceptance of the right of the law to dictate appropriate public behavior. When authorities possess legitimacy, they are better able to regulate effectively the behavior of citizens.[208]

With the birth of the UN and the change it brought to international law, the procedural authority to wage war shifted to the UN.[209] The UN, a new super-sovereign, limited just causes for war to defensive purposes and when "global peace and security" is threatened.[210] The UN's doctrine of the "responsibility to protect," which empowers the UNSC to intervene in states for humanitarian purposes, is an example of the UN taking away the power of sovereign states to go to war without defensive purposes, with the exception of allowing NSAs (freedom fighters) to fight for self-determination.[211]

Gentry argues that, because the Westphalian democratic structure is based on representation of its people, it should stay true even in non-Western contexts.[212] However, the liberal hermeneutic puts liberal voices above others and shuns other perspectives, thus ignoring events including colonialism, the Cold War, and the antihumanitarian aspects of the war on terror.[213] Therefore, she adds that, even as legitimate authorities, the Westphalian structure does not hold any moral authority which is required by ancient Greek philosophy of St. Augustine, who established that the authority needs to be divinely righteous.[214] St. Augustine believed that it is a "sovereign's responsibility to seek the good for the society he

---

[207] GENTRY, *supra* note 27, at 18. *Accord* MICHAEL WALZER, JUST AND UNJUST WARS: A MORAL ARGUMENT WITH HISTORICAL ILLUSTRATIONS (1977); ALEX J. BELLAMY, JUST WARS: FROM CICERO TO IRAQ (2006).

[208] T.R. Tyler, *Compliance and Obedience: Legal*, *in* INTERNATIONAL ENCYCLOPEDIA OF THE SOCIAL & BEHAVIORAL SCIENCES 2440, 2442 (Neil J. Smelser & Paul B. Baltes, eds., 2001).

[209] U.N. Charter art. 2, ¶ 4; *id.* arts. 39-51.

[210] U.N. Charter arts. 39-51.

[211] GENTRY, *supra* note 27, at 19.

[212] *See id.* at 20.

[213] *Id.*

[214] *Id.*

governs," yielding good results including peace, justice, and order.[215] In contrast, Luther argued that sovereignty belongs to secular states. Luther's secular view led to the Peace of Westphalia, which limited to states the sovereign authority to go to war and determined all actions of NSAs in this regard to be illegitimate. Gentry argues that Westphalian statehood creates injustice for marginalized populations in pursuit of social power.[216] Furthermore, according to Gentry, state moral legitimacy is a problem that leads to violence; NSAs that can govern their own territories should also be allowed sovereignty or rightful authority.[217]

Though the actions of a state are limited and controlled by customary norms, powerful nations with strong militaries and political power sometimes ignore these norms and harm weaker states. One example is the 2003 invasion of Iraq, where the United States invaded a sovereign country against the UNSC ruling. Such attacks in violation of the UN Charter's prohibition on the use of force are supported by scholars and writers, who construct narratives that favor a global system of state authority and Westphalian truths.[218] Even though the just war theory is based on the principle that legitimate authority to X rests with sovereign states, the majority of today's wars are fought by proxy NSAs.[219] Gentry explains that she does not call upon all NSAs to take up arms: instead, there can be amicable solutions when opposition to a state exists, like the support of Libyan rebels against Gaddafi or the Tamil people against the Sri Lankan government, derived from identity politics to end injustices.[220]

Gentry believes that political violence used by NSAs is no less than any violence by the state.[221] Yet, inconsistently, the hermeneutical

---

[215] *Id.* at 20–21.

[216] *Id.* at 21.

[217] *Id.* at 19–23.

[218] *See id.* at 20–23.

[219] *See* Candace Rondeax & David Sterman, *Twenty-First Century Proxy Warfare: Confronting Strategic Innovation in a Multipolar World Since the 2011 NATO Intervention, in* NEW AMERICA, Feb. 2019, at 40, 41, 52; Vladimir Rauta, *Toward a Typology of Non-State Actors in 'Hybrid Warfare': Proxy, Auxiliary, Surrogate and Affiliated Forces,* 32 CAMBRIDGE REV. INT'L AFF., Sept. 2019, AT 1; Vladyslav Lanovoy, *The Use of Force by Non-State Actors and the Limits of Attribution of Conduct*, 28 EUR. J. OF INT'L L. 565, 566 (2017). *See, e.g.,* Michael P. Scharf, *How the War Against ISIS Changed International Law,* 48 CASE W. RES. J. INT'L L. 15 (2016); Erica Dreyfus Borghard, Friends with Benefits? Power and Influence in Proxy Warfare (2014) (unpublished Ph.D. dissertation, Columbia University).

[220] *See* GENTRY, *supra* note 27.

[221] *See id.* at 23–24.

injustice deems state violence to be more legitimate than that of NSAs.[222] Hermeneutic injustice occurs when a marginalized group is not understood in a genuinely epistemic way and is considered not credible, just because it comes from the outside limits of the Westphalian system.[223] Gentry suggests that the term "terrorism" is itself ill-understood and processed out of anxiety and fear.[224] One's freedom fighter can be another's terrorist. For Gentry, deliberately targeting innocent people is one way to identify terrorists.[225]

A. DECONSTRUCTING GENTRY'S LEGITIMATE AUTHORITY

Though Gentry correctly identifies that legitimate authority is exclusive to states, which is supported by the Westphalian construct and Western scholarly narratives,[226] her argument fails to address why this is the case because it only relies on the notions of power and identity politics. If identity politics were the sole explanation, then legitimate authority suggested by Gentry to have a bias against Muslims would not have been extended to Islamic states. Yet, legitimacy is universal. For instance, the issue of "legitimate authority limited to only states" is not the creation of Westphalia. The concept had existed for centuries before, to deal with the principal-agent conundrum, in order to hold people and nations responsible for the actions taken. Gentry ignores the discussion of repercussions and the benefits of allowing legitimate authority to wage wars for NSAs. The only example she quotes pertains to antigovernment rebels who were installed by the West, the very thing her position was intended to counter.[227]

Gentry's legitimate authority argument is tied to moral grounds, which is not borne out given injustices undertaken by modern state actors.[228] Gentry's position inconsistently uses morality. For instance, she

---

[222] *See id.* at 24.

[223] MIRADA FRICKER, EPISTEMIC INJUSTICE: POWER AND THE ETHICS OF KNOWING 6–7 (2007).

[224] GENTRY, *supra* note 27.

[225] *Id.*

[226] *See id.* at 19, 21–22.

[227] Yet, once a sub-state group begins to arm, "terrorism" is most often the label given to it. A politically violent sub-state actor may receive international support if opposition to the regime already exists. Take, for instance, the support given to the Libyans against Muammar Gaddafi as opposed to fundamental lack of support granted to the Tamilese against the Sri Lankan state—both involve state-conducted genocidal acts and ethnic cleansing against sub-state actors. *Id.* at 24.

[228] *See id.* at 22–23.

believes that legitimate authority should not be limited to only states and should apply to NSAs, because states are not morally upright and commit injustices, and the international community grants legitimate authority to sub-state violent actors only when it suits them.[229] Her argument about legitimate authority is revealed to be contradictory when it addresses immoral acts by states. Illegitimate actions of a state (such as the US invasion of Iraq) cannot be reconciled with the notion that reserving legitimate authority for states is morally wrong. A breach of an established norm of just cause does not support an argument to discredit legitimate authority. Waging wars not justified in international law is a question of the notion of just cause and not of legitimate authority. It would have been a question of legitimate authority if, routinely, heads of state are somehow not true representatives of their people, an argument that has been used by Westerners against dictators.[230] While a dictatorship is not considered a legitimate authority by the West, international law considers it a legitimate authority. Gentry retreats from her own argument to allow all NSAs legitimate authority by advocating for the same powers for only freedom fighters. But that too, according to her, is allowed in international law.[231]

Gentry advances a realist argument when she says that NSAs should be allowed legitimate authority because, in practice, NSAs are fighting today's proxy wars.[232] A wrong committed outside the norms or accepted practices of customary international law, however, does not mean that the established norms are erroneous. A breach in the practice only means that the act itself is immoral and is in contradiction with international norms. For instance, the use of NSAs out of uniform and without the agency of a state is illegal under the international law addressing the use of force.[233] If NSAs are considered to have legitimate authority (as propounded by Gentry), legitimate authority would be extended to all of the residents in any given state. So, if Gentry's argument is accepted, it would mean that everyone on this planet has legitimate authority to use force inside or outside a state.

---

[229] *See id.* at 23–25.

[230] For instance, see anti-government support for Libyan rebels against Gaddafi by the West. *See generally* Martin Asser, *The Muammar Gaddafi Story*, BBC NEWS (Oct. 21, 2011), https://www.bbc.com/news/world-africa-12688033 [https://perma.cc/EBA3-WCMN].

[231] GENTRY, *supra* note 27.

[232] *Id*.

[233] Additional Protocol I, *supra* note 106, art. 44, ¶ 7.

If legitimate authority is granted to all NSAs, it will mean more support for rebels violating principles of nonintervention and harming the political sovereignty of states. This means that global peace and security will not only be threatened, it will be destroyed. Today, the only ideologies that restrict violence, armed conflicts, civil wars, and rebellions in the world are the principles of nonintervention, state sovereignty, and restrictions on using NSAs in other states.[234] Conferring legitimate authority on NSAs, as supported by Gentry, will mean discarding international law altogether.

If the notion of legitimate authority is extended to NSAs, this would allow NSAs to use force or challenge their own state for any reason. Granting NSAs legitimate authority will also foster their employment in cyberwarfare and international armed conflicts. NSAs already easily avoid retribution; granting them legitimate authority will likely increase their employability in proxy wars, as the use of NSAs in wars diffuses responsibility of armed attacks. There may have been a period where granting NSAs legitimate authority would not have created harm, but the best way to determine political power is by determining what does good for society. Violence is not the only way to resolve issues; it disproportionately affects the lives and livelihoods of innocent people.

Gentry does address some of the possible repercussions of allowing legitimate authority for NSAs. Gentry believes that the worries about chaos are misplaced because terrorists and violent NSAs are ill-understood in the epistemic injustice. Gentry believes that even the idea of considering terrorists as terrorists for deliberately targeting innocent people is problematic, since it is not universal and not applied to Western forces deliberately targeting innocent people.[235] Yes, soldiers fighting for a state can also be terrorists if they choose to violate humanitarian laws such as targeting a school full of innocent children on the pretext of securing the national interests of their state. But international law is already able to label states that allow this as violating international law. The very nature of humanitarian law is to make sure that the armed forces of a state do not intentionally harm civilians during wartime. If NSAs are allowed to have legitimate authority to use force in other states, the Geneva Conventions and humanitarian laws will not be able to protect innocent people due to the issue of the lack of retaliation towards NSAs. This is why the principal-agent conundrum is so crucial to this debate. The

---

[234] GENTRY, *supra* note 27, at 19–21.

[235] *See* GENTRY, *supra* note 27.

question arises as to who shall be held responsible for the atrocities and violence against innocent people if NSAs are allowed to wage wars against their own states or against other states through cyber warfare or by conventional means, while indiscriminately targeting combatants and noncombatants. Gentry ignored the moral problems by not discussing the repercussions of allowing legitimate authority for NSAs.

In sum, Gentry's idea of allowing legitimate authority for NSAs is erroneous and troublesome. The idea is troublesome because the idea resembles cyberwarfare tactics by avoiding possible attribution and retribution. Cyberwarfare, for instance, is mainly used to avoid any possible attribution.[236] So, the proposition of allocating legitimate authority for NSAs supports justification for the modern hybrid warfare techniques of aggressive states to be able to avoid attribution and retribution. Therefore, extending legitimate authority to NSAs would disrupt global peace and security by provoking unnecessary violence and fail to hold all the perpetrators of violence responsible by disregarding the principal-agent conundrum.[237] Moreover, the realist arguments of misuse of power, the occurrence of injustice, and breaches of established norms are not adequate to discredit the notion of reserving legitimate authority to states. This support for states' monopoly on legitimate authority to use force is not, as assumed by Gentry, for the power to marginalize terrorists or to do hermeneutic injustice to fundamentalists. Instead, the epistemic support for the use of NSAs and cyber tactics is to avoid attribution, which is biased in favor of power politics and in support of aggression. A better argument might have been explaining how this injustice is inflicted upon terrorists, and how using force by NSAs is absolutely necessary, without merely arguing that the state monopoly on legitimacy is a Westphalian construct that ill-understands terrorists or violent NSAs. It's not clear that Gentry could provide any salient examples, aside from that Libyan rebels destabilized Libya.[238] Furthermore, the US aided Libyan rebels, but the movement was not entirely orchestrated by the US.[239]

---

[236] Rid, *supra* note 159, at 15–16.

[237] COKER, *supra* note 80.

[238] GENTRY, *supra* note 27, at 24.

[239] Gabriel Moyssen, *Regime Change Failure: Libya's 8-Year Long Civil War Comes to Tripoli*, EL UNIVERSAL (Mex.), Apr. 12, 2019, https://www.eluniversal.com.mx/english/regime-change-failure-libyas-8-year-long-civil-war-comes-tripoli [https://perma.cc/RB85-KF9W].

IV. CONCLUSION

The current just war theory is not perfect and can certainly be improved. As a result, the notion of jus post bellum[240] has been gaining traction in recent times. This theory argues that just war theory should extend beyond the end of war. It should continue to protect the rights and sovereignty of defeated states, even after war is over.[241] Dubik argues that jus in bello restricts violence against innocent people, but there is still a missing piece.[242] He argues that jus in bello or humanitarian law only judges warfare in action at the tactical level, where only pawns are involved, and where military necessity and collateral damage can justify violation of humanitarian law in particular situations. In addition, he adds, jus in bello should consider monitoring wars at the strategic level, where the real game-changing plans are made.[243]

In cyberwarfare, Yorum Dinstein and Daniel Silver are also of the view that cyberattacks that produce the same result as kinetic weapons should be considered a use of force or an armed attack.[244] Based on these arguments and the *opinio juris* of the UN members, the UNGA report of 2013 concluded that cyberattacks can be considered a use of force. The report said that "international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT [Information and Communications Technologies] environment."[245] However, the report sets criteria for categorizing cyberattacks for this purpose: the cyberattacks must be attributable to a state; the effect of the cyberattack must be equivalent to the conventional use of force, such as causing destruction to life or property; and a cyberattack must be international in nature, violating the sovereignty of a state.[246]

While assessing the future of just war theory, Caron Gentry,[247] along with Virginia Held[248] and Tarik Kochi,[249] argue that there is an

---

[240] FROWE & LANG, *supra* note 10.
[241] *Id.*
[242] *See* Dubik, *supra* note 14, at 11, 14.
[243] *Id.* at 13–15, 20.
[244] Yourum Dinstein, *Computer Network Attacks and Self-Defense*, 76 INT'L L. STUD. 99, 103 (2001).
[245] Developments in Information and Telecommunications, *supra* note 144, at 8.
[246] *See* Roscini, *supra* note 153, at 234.
[247] *See* GENTRY, *supra* note 27.
[248] HELD, *supra* note 195. *See also* GENTRY, *supra* note 27, at 25.
[249] Kochi, *supra* note 196. *See also* GENTRY, *supra* note 27, at 25–26.

international bias toward the established notion of lending political and moral legitimacy of authority to states to wage wars. The use of force by NSAs as legitimate authority can only be considered in limited circumstances in domestic law, and especially in instances of colonized states (wronged or oppressed by other states, such as in Palestine).[250] But, to a larger extent, the legitimate authority to use force vests in states or heads of state.[251] In addition to its utility in the principal-agent problem,[252] limiting legitimate authority only to states serves to maintain states' monopoly on the use of force.[253] This way, the status quo within a state, as well as the global order, are both maintained. While some may argue that destruction would ensue if NSAs were given legitimate authority to use force, others support the view that legitimate authority should be allowed for NSAs in the future.[254] This is understandable, because NSAs (including terrorists, mercenaries, and rebel groups) are pawns employed by states for their proxy wars and asymmetric tactics.[255] NSAs' utility in asymmetric warfare is high because their use avoids attribution and retribution,[256] and they are cheaper to maintain than conventional armed forces.[257]

However, the idea of allowing legitimate authority for NSAs such as rebel groups, mercenaries, and terrorists is erroneous and troublesome. The legitimate authority for NSA would not only destroy global peace and security by creating unnecessary violence, bloodshed, and wars, but also exonerate all the perpetrators of violence by ignoring the principal-agent conundrum.[258] Moreover, the realist argument regarding the misuse of power, occurrence of injustice, and breaches of established norms are not sufficient to discredit the perception of legitimate authority only for states. It is not—as assumed by Gentry—for power politics, to marginalize terrorists, or to do hermeneutic injustice to fundamentalists.

---

[250] Coverdale, *supra* note 33, at 250–51.

[251] *Id.*

[252] *See* COKER, *supra* note 80, at 65. *See also* CARMOLA, *supra* note 73, at 138.

[253] Schwekenbecher, *supra* note 81, at 161–62.

[254] *See* GENTRY, *supra* note 27.

[255] Scott, *supra* note 22, at 6. *See also* Śliwa et al., *supra* note 22, at 90. NATO, *supra* note 22, at 10–11. Ashraf, *supra* note 22, at 14. European Commission, *supra* note 22.

[256] Scott, *supra* note 22, at 6; Śliwa et al., *supra* note 22, at 95; NATO, *supra* note 22, at 25. Ashraf, *supra* note 22, at 14.

[257] MCFATE, *supra* note 86, at 125.

[258] COKER, *supra* note 80, at 65; CARMOLA, *supra* note 73, at 138.

In a nutshell, just war theory was developed to support individual state sovereignty, to protect the universal status quo, and to maintain global peace and security.[259] It allows the use of armed force in self-defense and under UNSC authorization.[260] Only states can make a decision to use legitimate force during wars.[261] Moreover, to restrict violence, and to safeguard the peace and security of this world, resorting to the use of force must be the last resort after exhausting all the peaceful solutions.[262] This means that the contemporary legal framework of international law intends to foster peace. This reasoning is also supported by the fact that humanitarian law under jus in bello also protects innocent lives during armed conflicts.[263]

States constantly formulate new means to justify their aggression, including by employing modern warfare tactics where the attribution and retribution of armed attacks are avoided.[264] The use of information warfare and the employment of NSAs as proxy warriors in modern conflicts are some examples of such tactics that evade the existing framework of just war theory.[265] If cyberattacks are not considered a use of force, there will be a lacuna in the international legal system that can be easily exploited by the states. The rule of thumb is that states can retaliate proportionally against cyberattacks, and the defensive use of conventional force by victim states is only allowed when the threshold of damage of a cyberattack is equivalent to that of the conventional use of armed force.[266] Similar to the use of cyberattacks by countries, NSAs are also employed as proxy warriors to avoid attribution and retribution. If legitimate authority as propounded by Gentry is extended to NSAs, it will lead to the legalization of covert use of mercenaries, terrorists, and proxy warriors by states. It may also encourage other states to turn a blind eye to their use. More importantly, if NSAs such as terrorists are afforded the legitimate authority to employ violence—as an inverse effect—it will legitimize terrorism. In

---

[259] Coverdale, *supra* note 33, at 234–235.

[260] U.N. Charter art. 2, ¶ 4; *id.* arts. 39–43, 51.

[261] COKER, *supra* note 80, at 65.

[262] *See* SCHWENKENBECHER, *supra* note 94, at 85.

[263] Additional Protocol I, *supra* note 106, art. 19. *See also* IV Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1959, 75 U.N.T.S 287.

[264] Scott, *supra* note 22, at 6; Śliwa et al., *supra* note 22, at 96; NATO, *supra* note 22, at 11–25; Ashraf, *supra* note 22, at 14; European Commission, *supra* note 22.

[265] Klamberg, *supra* note 192, at 189.

[266] CORTEN, *supra* note 161, at 55, 66–67. *See also* Koh, *supra* note 156, at 593–95.

a sense, this requirement of legitimacy for NSAs is a vehicle of moral and legal tour de force against terrorism.[267] The prohibition on the use of force, and the principle of non-intervention are flexible enough to face modern emerging war tactics. Moreover, the state monopoly on legitimate authority to use force is crucial to keep the principal-agent problem in check, so that people responsible for any violence can be held accountable.[268] For these reasons, the future of just war theory should not include legitimate authority for NSAs, and it should include cyberattacks within the confines of the prohibition on the use of force under Article 2(4) of the UN Charter.

[267] CAMPOS, *supra* note 82, at 90–91.
[268] CARMOLA, *supra* note 73, at 138.