REVISITING BELLIGERENT REPRISALS IN THE AGE OF CYBER?

DAVID WALLACE, SHANE REEVES & TRENT POWELL*

I. INTRODUCTION

With respect to current and future warfare, it is virtually impossible to exaggerate the significance of information technology. Today's armed forces use a host of weapons, munitions, and systems that function through the operation of highly sophisticated information systems.[1] For instance, the command and control of operational forces are increasingly coordinated and directed through computer-based networks that allow for real-time sharing of information and common pictures of the battlespace.[2] Moreover, logistics, at all levels of warfare, are entirely at the mercy of information systems. And, of

* Colonel David Wallace is the Professor and Head, Department of Law, United States Military Academy at West Point, New York. In 2017, Colonel Wallace served as a Visiting Scholar at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia. The author would like to thank the NATO CCDCOE Director, Merle Maigre, the Law Branch Chief, Lauri Aasmann, and all of the members of the Law Branch for their collegial assistance and support during the fellowship. Lieutenant Colonel Shane Reeves is the Professor and Deputy Head, Department of Law, United States Military Academy at West Point, New York. He is an Associate Professor of Law. Major Trent Powell is serving as an action officer in the Future Concepts Directorate at The Judge Advocate General's Legal Center & School. Major Powell previously served as an Assistant Professor of Law, Department of Law, United States Military Academy at West Point, New York. The opinions, conclusions, and recommendations in this article do not necessarily reflect the views of the Department of Defense, the United States Army, or the United States Military Academy.

1. COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 9 (William A. Owens et al. eds., 2009).

2. *Id.*

course, in recent years the development of cutting edge, high-tech cyber weapons allow for an attack against an adversary in both virtual and real domains.[3] While this "New Age of Cyber" may seem to raise questions about the legal framework applicable to the conduct of such operations, the traditional normative legal structure for warfare, the *jus ad bellum*[4] and the *jus in bello*,[5] still regulate the actions of belligerents engaged in cyber hostilities.

This article deals with legal issues in the cyber warfare context related to the *jus in bello*, which is also referred to as international humanitarian law (IHL). The international legal community acknowledges and widely accepts that IHL applies to cyber operations undertaken in the context of an armed conflict.[6] The challenge, of course, is not that IHL applies, but rather how it specifically applies to cyber operations. Unquestionably, digital means and methods of warfare executed in both the virtual and real world pose novel issues.[7] In this regard, it is necessary to consider and examine how pre-cyber IHL laws, as well as the values that formed the foundation for those laws,[8] translate into regulation of armed conflicts in the New Age of Cyber. Although there are many issues and topics that are worthy of such a re-examination, few are as controversial as the notion of belligerent reprisals under IHL.

As will be discussed in detail below, a belligerent reprisal under IHL is a method of warfare that is otherwise unlawful but, in exceptional cases, is lawful when used as an enforcement mechanism in response to unlawful enemy acts.[9] As noted by Professor William Schabas, "[r]eprisal amounts to an argument that crimes are justifiable as a proportionate response to criminal acts committed by the other party. In a sense, it is the most ancient means of

3. *Id.* at 10.

4. *Jus ad bellum* addresses when a State may use force under international law. *What are* Jus ad bellum *and* Jus in bello*?* INT'L COMM. RED CROSS, https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0 [https://perma.cc/7AP3-7D8M] (last visited Nov. 7, 2017). Some legal commentators have observed that the United Nations Charter creates a legal regime more accurately characterized as *jus contra bellum* because it is fundamentally devised to prevent the use of force. *See* ROBERT KOLB & RICHARD HYDE, AN INTRODUCTION TO THE INTERNATIONAL LAW OF ARMED CONFLICTS 13 (2008).

5. The *jus in bello* regulates the conduct of parties engaged in an armed conflict. *See What are Jus ad bellum and Jus in bello?*, *supra* note 4.

6. *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 3 (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0].

7. *See, e.g.*, David Wallace & Shane R. Reeves, *The Law of Armed Conflict's "Wicked" Problem:* Levée en Masse *in Cyber Warfare*, 89 INT'L L. STUD. 646, 666–67 (2013) (discussing the difficulty of applying the traditional IHL interpretation of a *levée en masse* in the cyber domain).

8. HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR 239–40 (James Crawford & John S. Bell eds., 2012).

9. 1 JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW: RULES 513 (2005).

enforcement of the law."[10] Under this assertion, then, a "proportionate response" by an aggrieved party serves as a *jus in bello* enforcement of the law. And, because the enforcement of international law and IHL specifically, is the obvious shortcoming with international law, belligerent reprisals may provide a timely mechanism to redress enemy violations of IHL *during* the armed conflict itself.[11]

The use of belligerent reprisal has evolved over time "from a fundamental and nearly universally recognized aspect of the international law" regulating warfare "into a complex and [highly] contentious sanction."[12] Arguably, in modern IHL, reprisals have been largely—but not entirely—prohibited by customary and codified law. The 1977 Additional Protocols (AP) I[13] is unquestionably the international community's strongest and most comprehensive condemnation of belligerent reprisals as a method of warfare. Commenting on the efforts that led to AP I, Konstantin Obradovic, who took part in the Diplomatic Conference of 1974–1977 as a member of the Yugoslav delegation, made the following observations about belligerent reprisals:

> With its well-nigh absolute prohibition of reprisals against all categories of protected persons who fall into enemy hands, Protocol I goes further down the trail blazed in 1949. The underlying considerations are both humanitarian and rational. The history of war—and the Second World War in particular—clearly shows that, apart from being barbarous, unfair and inequitable as they invariably victimize the innocent, reprisals achieve nothing. Even if they are 'justified' as a response to enemy violation of the law, they never result in the triumph of the rule of law. Moreover, all the mass executions of the last world war, all the Oradour-sur-Glane of this world have not been enough to dampen people's determination to resist. Reprisals therefore appear pointless.[14]

10. GARY D. SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR 693 (2d ed. 2016) (quoting WILLIAM A. SCHABAS, THE INTERNATIONAL CRIMINAL COURT: A COMMENTARY ON THE ROME STATUTE 496 (2010)).

11. A.P.V. ROGERS, LAW ON THE BATTLEFIELD 14 (2d ed. 2004). Importantly, reprisals are separate and distinct from acts of retaliation and revenge, which remain unlawful under IHL. GEOFFREY BEST, HUMANITY IN WARFARE 19 (1980).

12. Sean Watts, *Reciprocity and the Law of War*, 50 HARV. INT'L L.J. 365, 382 (2009).

13. Protocols Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Jun. 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I].

14. Konstantin Obradovic, *The Prohibition of Reprisals in Protocol I: Greater Protection for War Victims*, INT'L REV. RED CROSS, Oct. 31, 1997, at 524, https://www.icrc.org/eng/resources/documents/article/other/57jnv7.htm [https://perma.cc/FY6J-PF9P].

While Obradovic expressed this view at the earliest period in the development of cyber capabilities, the current and future state of reprisals in the cyber realm require a review of more recent legal analysis. In that regard, a useful starting point for legal practitioners, policymakers, non-governmental organizations,[15] cyber security professionals, military commanders, and scholars is the 2017 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (*Tallinn Manual 2.0*).[16] This resource, which is best understood as the collective opinions of a group of international experts, helpfully addresses the question of belligerent reprisals under IHL in armed conflict as well as many other vital issues spanning public international law in its nearly 600 pages of highly informative text.[17] Impressively, *Tallinn Manual 2.0* has 154 rules including two rules on reprisals: Rule 108, *Belligerent Reprisals*, and Rule 109, *Reprisals under Additional Protocol I*.[18] In addition to the actual rules contained in *Tallinn Manual 2.0*, the manual provides detailed commentary, offering some tremendously valuable insights into the normative context of the rules as well as practical implications for their application.[19] Finally, and most importantly, it is important to note that the experts who wrote *Tallinn Manual 2.0* were limiting themselves to an objective restatement of the *lex lata* and scrupulously avoided including statements reflecting the *lex ferenda*.[20]

This article critically explores the legal landscape of belligerent reprisals and considers whether the use of these measures is a viable enforcement mechanism under IHL in the context of cyber operations. Because of the layered approach to this inquiry, the article has seven parts that build upon each other. Part II of the article provides an overview of the history of belligerent reprisals under IHL. Part III discusses belligerent reprisals in the context of today's understanding of IHL. Part IV further explores cyber operations and belligerent reprisals: the *lex lata*. Countermeasures (at one time known as peacetime reprisals) under the law of state responsibility forms the basis of Part V. Part VI provides an analytical framework for considering how cyber means

15. An example of one such non-governmental organization is the ICRC. *The ICRC's Mandate and Mission*, INT'L COMM. RED CROSS, https://www.icrc.org/en/mandate-and-mission [https://perma.cc/XQM3-32BJ] (last visited Dec. 6, 2017). The ICRC is an "independent, neutral organization ensuring humanitarian protection and assistance for victims of armed conflict and other situations of violence. It takes action in response to emergencies and at the same time promotes respect for international humanitarian law and its implementation in national law." *Id.*

16. TALLINN MANUAL 2.0, *supra* note 6.

17. *See id.*

18. *Id.* at 460–63.

19. *Id.* at 3–5.

20. *Id.* at 3.

and methods could effectively facilitate an expanded use of belligerent reprisals for some States under some conditions. Additionally, this section serves as the lens for re-examining the propriety and practicality of breathing life back into this controversial enforcement mechanism under IHL. Lastly, Part VII summarizes and concludes the article.

II. THE HISTORY OF BELLIGERENT REPRISALS IN IHL

Reprisals have been the traditional method of enforcement of IHL since at least the late nineteenth and early twentieth centuries.[21] This time period saw a number of advances in IHL including the adoption of the first Geneva Convention; the St. Petersburg's Declaration, which renounced the use of exploding bullets projectiles under 400 grams; and the drafting and implementation of the so-called Lieber Code[22] during the American Civil War.[23] The 1863 Lieber Code addressed the concept of reprisals throughout its 157 articles.[24] Notably, Francis Lieber, the Code's main architect and drafter, described "retaliation"—which was used synonymously with the term "reprisals"—as the sternest feature of war.[25] Article 28 of the Code states:

> Art. 28. Retaliation will, therefore, never be resorted to as a measure of mere revenge, but only as a means of protective retribution, and moreover, cautiously and unavoidably; that is to say, retaliation shall only be resorted to after careful inquiry into the real occurrence, and the character of the misdeeds that may demand retribution. Unjust or inconsiderate retaliation removes the belligerents farther and farther from the mitigating rules of regular war, and by rapid steps leads them nearer to the internecine wars of savages.[26]

During the American Civil War reprisals were a lawful method of enforcing the laws and customs of war with both sides making abundant use of the method.[27] The Lieber Code even permitted retaliation against prisoners of war

21. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 514.

22. SOLIS, *supra* note 10, at 44–45. In 1862, the War Department appointed a board of officers, including Francis Lieber, to propose a "Code of Regulations for the government of armies in the field." *Id*. The military officers on the board worked primarily on a revision to the Articles of War. *Id*. Francis Lieber, a professor at Columbia, wrote the Code that bears his name. *Id*. In 1863, President Lincoln directed that Lieber's 157-article Code be incorporated into the Union Army's General Orders as "General Order 100." *Id*.

23. *Id*. at 43.

24. *See* General Orders No. 100: Instructions for the Government Armies of the United States in the Field (Apr. 24, 1863) [hereinafter *Lieber Code*].

25. *Id*. art.27.

26. *Id*. art.28.

27. Patryk I. Labuda, *The Lieber Code, Retaliation and the Origins of International Criminal*

("[a]ll prisoners of war are liable to the infliction of retaliatory measures.").[28] In only the instance of later capture and execution of deserters joining an enemy army did the Lieber Code forbid retaliation.[29]

Despite the Lieber Code's statement on the lawfulness of reprisals, other legal bodies sought to limit the use of reprisals. The Brussels Conference of 1874 and the Institute of International Law meeting at Oxford in 1880 were two such instances.[30] The Institute's Manual of the Laws of War on Land stated that reprisals "must conform in all cases to the laws of humanity and morality."[31] However, the Hague Conventions at the turn of the twentieth century did not prohibit the use of belligerent reprisals apart from providing some rudimentary protections for prisoners of war.[32] In fact, during early armed conflicts of the twentieth century, air attacks were a legitimate means and method of reprisal against a defaulting enemy to bring it back to its senses.[33] Commenting on this phenomenon, Air Commodore William Boothby stated:

> The civilian population and the popular press would demand retaliatory or reprisal action against the enemy in response to air raids that occasioned civilian loss. Air raids carried out as reprisal action could be portrayed by the adverse party as simple illegal acts ignoring, of course, the alleged prior illegality cited as justifying the reprisal in the first place.[34]

Reprisals in World War I caused much hardship for the victims of the conflict and, in particular, prisoners of war. As a result, the idea of prohibiting all reprisals against prisoners of war gained traction, eventually finding official endorsement in special agreements concluded between parties to the conflict

---

Law, *in* 3 HISTORICAL ORIGINS OF INTERNATIONAL CRIMINAL LAW 299, 304, 306 (Morten Bergsmo et al. eds., 2015).

28. *Lieber Code*, *supra* note 24, art.59.

29. *Id.* art.48. This provision specifically states:

> Deserters from the American Army, having entered the service of the enemy, suffer death if they fall again into the hands of the United States, whether by capture, or being delivered up to the American Army; and if a deserter from the enemy, having taken service in the Army of the United States, is captured by the enemy, and punished by them with death or otherwise, it is not a breach against the law and usages of war, requiring redress or retaliation.

Id.

30. *See* Project of an International Declaration Concerning the Laws and Customs of War, Brussels, Aug. 27, 1874, https://ihl-databases.icrc.org/ihl/INTRO/135 [https://perma.cc/Q5VC-QGC8]; The Laws of War on Land, Oxford, Sept. 9, 1880, https://ihl-databases.icrc.org/ihl/INTRO/140?OpenDocument [https://perma.cc/M2FJ-AG3G].

31. The Laws of War on Land, *supra* note 30, art.86.

32. INGRID DETTER, THE LAW OF WAR 301 (2d ed. 2000).

33. WILLIAM H. BOOTHBY, THE LAW OF TARGETING 512 (2012).

34. *Id.* at 512–13.

towards the end of the war.[35] Following World War I, the 1929 Geneva Convention on Prisoners of War began the process of gradually excluding groups of persons and civilians' property from the scope of reprisals,[36] including prisoners of war.[37] Commenting on this particular category, Michael Walzer, in his classic book *Just and Unjust Wars*, stated, "prisoners were singled out because of the implied contract by surrender, in which they are promised life and benevolent quarantine. Killing them would be a breach of faith as well as a violation of the positive laws of war."[38]

Despite these efforts, World War II saw the regular use of reprisals by the parties to the conflict.[39] There were a number of well-known incidents involving reprisals including one involving the Germans and the French resistance fighters in 1944.[40] After the Normandy invasion, French resistance fighters organized into the French Forces on the Interior (FFI) and began operating openly and on a larger scale.[41] They wore insignia visible at a distance, carried their arms openly, and abided by the laws and customs of war, thereby qualifying them as lawful combatants.[42] However, the Germans did not recognize the FFI as lawful combatants.[43] Rather, the Germans viewed them as criminals and summarily executed a number of FFI fighters upon capture.[44]

By the late summer of 1944, "many German soldiers had surrendered to the FFI."[45] When the FFI learned the Germans executed eighty FFI fighters and planned to execute more, "the FFI announced that it would carry out eighty reprisal executions."[46] The International Committee of the Red Cross (ICRC)

35. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=8F88DE5EE5DEA183C12563CD0042207D [https://perma.cc/P7T2-57TR].

36. THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 234 (Dieter Fleck ed., 3d ed. 2013).

37. Convention Relative to the Treatment of Prisoners of War, Geneva, July 27, 1929, Art. 2, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/ART/305-430003?OpenDocument [https://perma.cc/244B-DFX9].

38. MICHAEL WALZER, JUST AND UNJUST WARS: A MORAL ARGUMENT WITH HISTORICAL ILLUSTRATIONS 209 (4th ed. 2006).

39. DETTER, *supra* note 32, at 301.

40. Kenneth Anderson, *Reprisal Killings*, *in* CRIMES OF WAR 2.0: WHAT THE PUBLIC SHOULD KNOW 358, 358–59 (Roy Gutman, David Rieff & Anthony Dworkin eds., 2007).

41. *Id*. at 358.

42. *Id.*

43. *Id.*

44. *Id.*

45. *Id.*

46. *Id.*

intervened and sought to postpone the executions pending an agreement whereby the Germans would recognize the FFI as lawful combatants.[47] But, after six days in which the Germans did not respond, the FFI executed eighty German prisoners.[48] Subsequently, the historical accounts indicate the Germans abandoned any plans to execute additional FFI prisoners.[49]

In addition to the actual use of reprisals by parties in World War II, there was also the threatened use of belligerent reprisals. For example, President Franklin Roosevelt threatened the use of retaliatory attacks upon becoming aware that Axis forces sought to use poison gas.[50] The regular use, or threat of use, of belligerent reprisals in World War II thus became an important topic in the post-war tribunals. Commenting about the scope of belligerent reprisals, the International Military Tribunal found that:

> The right of reprisals against civilians was restricted by rules laid down in the judgments of the Military Tribunal at Nuremberg. The Tribunal emphasised that reprisals must at least be limited geographically to one area, mainly as action against persons in one area could have little deterrent effect on people in other areas. If there was not such geographical connection a 'functional' link might be acceptable as limiting the right of reprisals: there had thus to be some connection between the reprisals and the civilians against whom action was taken. The Tribunal furthermore ruled out reprisals for which certain ethnic, religious or political groups had been selected.[51]

On August 12, 1949, a diplomatic conference in Geneva approved the text of four conventions to which more States have ratified than any other international agreements in the laws regulating armed conflict: the 1949

47. *Id.*

48. *Id.*

49. *Id.*

50. Andrew D. Mitchell, *Does One Illegality Merit Another? The Law of Belligerent Reprisals in International Law*, 170 MIL. L. REV. 155, 171 (2001). President Roosevelt specifically stated:

> [T]here have been reports that one or more of the Axis powers were seriously contemplating use of poisonous or noxious gases or other inhumane devices of warfare. . . . We promise to any perpetrators of such crimes full and swift retaliation in kind. . . . Any use of gas by any Axis power, therefore, will immediately be followed by the fullest possible retaliation upon munition centers, seaports, and other military objectives throughout the whole extent of the territory of such Axis country.

Id. (alteration in original).

51. DETTER, *supra* note 32, at 301.

Geneva Conventions.[52] The Conventions were, in part, born out of the unprecedented brutality and violence of World War II.[53] As Ambassador George H. Aldrich commented:

> The history of development of this branch of international law is largely one of reaction to bad experience. After each major war, the survivors negotiate rules for the next war that they would, in retrospect, like to have seen in force during the last war. The 1929 and 1949 Geneva Conventions attest to that pattern.[54]

The four Conventions prohibited belligerent reprisals with respect to the specific classes of individuals covered by each agreement: wounded, sick, and shipwrecked; medical and religious personnel; prisoners of war; civilians in occupied territories; as well as certain objects such as medical facilities and supplies and private property of civilians in occupied territory.[55] Adding to

52. ADAM ROBERTS & RICHARD GUELFF, DOCUMENTS ON THE LAWS OF WAR 195 (3d ed. 2000). To provide some background and context, the Geneva Conventions may be traced back to a well-to-do Swiss businessman, Henri Dunant, and the Battle of Solferino in 1859. *Solferino and the International Committee of the Red Cross*, INT'L COMM. RED CROSS, https://www.icrc.org/eng/resources/documents/feature/2010/solferino-feature-240609.htm [https://perma.cc/KC3E-SDEH] (last visited Jan. 3, 2018). The Battle of Solferino in Lombardy, not far from Milan and Verona, was fought between the forces of Austria and a French-Piedmontese alliance. *Id*. The battle was one of the bloodiest of the nineteenth century with thousands of dead and wounded on both sides. *Id*. The military practice of the time was to leave the wounded where they had fallen on the battlefield. *Id*. Dunant was there and witnessed the carnage and participated in the aftermath attempting to provide aid and comfort to survivors. *Id*. Dunant could not forget what he saw and experienced. *Id*. He published in 1862 a small book, *A Memory of Solferino*. *Id*. In the book, Dunant vividly and graphically described the battle and the suffering of the wounded and injured soldiers. *Id*. Additionally, in the book, Dunant called for the creation of relief societies in each country that would act as auxiliaries to the army medical services to facilitate the care for all wounded and sick, whichever side they were on. *Id*. This effort led eventually to the formation of the International Committee of the Red Cross. *Id*. Also, as part of Dunant's vision in *A Memory of Solferino*, he proposed that an international principle be created to serve as the basis for these societies. *Id*. Dunant's idea ultimately led to the Swiss government hosting an official diplomatic conference in August 1864, which resulted in the adoption of the first Geneva Convention. *Id*. In 1901, Dunant was awarded the first-ever Nobel Peace Prize for what was accurately described as the "supreme humanitarian achievement of the 19th century." *Id*.

53. *See* Phillip Spoerri, Dir. of Int'l Law, Int'l Comm. of the Red Cross, Address at Ceremony to Celebrate 60th Anniversary of the Geneva Conventions: The Geneva Conventions of 1949: Origins and Current Significance (Dec. 8, 2009), https://www.icrc.org/eng/resources/documents/statement/geneva-conventions-statement-120809.htm [https://perma.cc/2QXP-FPQ8].

54. SOLIS, *supra* note 10, at 88.

55. THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW, *supra* note 36, at 234, 334.

these prohibitions, the 1954 Hague Convention on the Protection of Cultural Property prohibited reprisals against objects protected under the convention.[56]

The 1977 AP I significantly enlarged the traditional prohibitions of reprisals under IHL adding several other categories of prohibited reprisal targets.[57] In addition to a general prohibition, AP I also specifically prohibits reprisals against the civilian population and objects; cultural property and places of worship; objects indispensable to the survival of the civilian populations; the natural environment; and works or installations containing dangerous forces.[58] However, the United States, as well as several other States, objected to these additional restrictions on reprisals as being counterproductive.[59]

Specifically, the United States argued AP I's greater prohibition on reprisals removed a significant tool for protecting civilians and war victims on all sides of a conflict.[60] For example, article 51 of the Protocol "prohibits any reprisal attacks against the civilian population, that is, attacks that would otherwise be forbidden but that are in response to the enemy's own violations of the law and are intended to deter future violations."[61] Yet, historically, reprisals were the major sanction underlying the laws of war and ensured reciprocal compliance.[62] "If article 51 were to come into force for the United States, an enemy could deliberately carry out attacks against friendly civilian populations, and the United States would be legally forbidden to reply in kind."[63] As a result, "[t]o formally renounce even the option of such attacks" would "remove a significant deterrent" for those intent on targeting unfriendly

56. *Id*. at 434; *see also* Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict, May 14, 1954, 249 U.N.T.S. 240, 244–48.

57. TALLINN MANUAL 2.0, *supra* note 6, at 463.

58. *Id.*

59. GEOFFREY S. CORN ET AL., THE LAW OF ARMED CONFLICT: AN OPERATIONAL APPROACH 227 (2012). In fact, the United States's objections concerning reprisals was one of the reasons it did not ratify AP I. *See* SOLIS, *supra* note 10, at 128–38; *see also* Michael J. Matheson, Deputy Legal Adviser, U.S. Dep't of State, Remarks at American Red Cross-Washington College of Law Conference on International Humanitarian Law (Jan. 22, 1987), *in* 2 AM. U. J. INT'L L. & POL'Y 419, 426 (1987).

60. OFFICE OF THE GEN. COUNSEL, U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL § 18.18.3.4, at 1088–89 (2016) [hereinafter LAW OF WAR MANUAL].

61. *Id*. § 18.18.3.4, at 1089 n.221 (quoting Judge Abraham D. Sofaer, Legal Adviser, U.S. Dep't of State, Remarks at American Red Cross-Washington College of Law Conference on International Humanitarian Law (Jan. 22, 1987), *in* 2 AM. U. J. INT'L L. & POL'Y 460, 469 (1987)).

62. *See* Watts, *supra* note 12, at 382.

63. LAW OF WAR MANUAL, *supra* note 60, § 18.18.3.4, at 1089 n.221 (quoting Sofaer, *supra* note 61, at 469).

civilian populations.[64] Today, the United States continues to hold, as an option, the use of reprisals in limited circumstances.[65]

III. BELLIGERENT REPRISALS TODAY IN IHL

As is evident from the above, the historical development of reprisals under IHL established a gradual trend to outlaw the practice.[66] There are, however, several important considerations with respect to reprisals under the present IHL framework. First, as a threshold matter, to the degree that a reprisal would be lawful today, they are subject to stringent controls.[67] Second, the concept of belligerent reprisals exists in the context of international armed conflicts and not in non-international armed conflicts.[68] And third, under customary IHL, there are six general conditions precedent to lawfully employing belligerent reprisals.[69]

The first condition relates to the purpose of reprisals.[70] As mentioned previously, the use of reprisals is only in reaction to a prior serious violation of IHL and done for the purpose of inducing the enemy to comply with IHL.[71] In many respects, this is the *sine qua non* of reprisals, i.e., to induce a law-breaking State to abide by IHL in the future.[72] Of course, in practice, determining motive for particular actions may be problematic. That is, it may be very difficult to discern whether there is a legitimate purpose for an action, i.e., inducing an adversary to comply with the law, or whether an act is actually retaliation, retribution, or revenge.[73] Additionally, because of the underlying purpose of belligerent reprisals, anticipatory or counter reprisals are impermissible.[74]

The second condition is that the employment of belligerent reprisals is a matter of last resort, and there must be no other lawful measures available to induce the enemy to respect and comply with IHL.[75] Before using reprisals,

64. *Id.* (quoting Sofaer, *supra* note 61, at 469).

65. *See* CORN ET AL., *supra* note 59, at 227.

66. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 513–14.

67. *Id.* at 513.

68. TALLINN MANUAL 2.0, *supra* note 6, at 464. The ICRC, in Rule 148 of its Customary International Law Study takes the position that parties to non-international armed conflicts do not have the right to resort to belligerent reprisals. *See* HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 526.

69. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 515–18; *see also* LAW OF WAR MANUAL, *supra* note 60, § 18.18.2.5, at 1086.

70. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 515.

71. *Id.*

72. *Id.* at 515–16.

73. BEST, *supra* note 11, at 167.

74. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 515.

75. *Id.* at 516.

States must first attempt to secure the enemy's compliance with IHL through certain means.[76] For example, actions such as "protests and demands, retorsion, or reasonable notice of the threat to use reprisals" are necessary before resorting to belligerent reprisals.[77] Notably, both international and domestic courts require meeting this condition prior to utilizing reprisals.[78]

The third condition is proportionality.[79] Proportionality has multiple meanings in international law. Generally, within the context of customary IHL, proportionality is understood to mean that an attack is prohibited if the incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, is "excessive in relation to the concrete and direct military advantage anticipated."[80] By contrast, in the context of belligerent reprisals, most State practices illustrate that the acts taken in reprisal be proportionate to the original violation, free from the balancing approach under the prevalent proportionality notion.[81]

In practice, proportionality may be hard to gauge in nature and scope, although it does not mean equivalence. Rather, it should be construed to mean the response should not be excessive.[82] Additionally, it is important to note that the proportionality requirement does not mean that the belligerent reprisal needs to be in kind.[83] For example, if State A bombs civilian objects in State B, State B is not limited to only bombing civilian objects in State A. In fact, there are many scenarios where there is not a direct counterpart to the original violation or the victim State may simply lack the technical expertise to respond in the same fashion.[84]

The fourth condition is somewhat straightforward and self-explanatory. Because reprisals are significant military and political acts that require careful and complex judgments, the law withholds authority to exact reprisals to the highest levels of government within a State.[85] As noted by one legal commentator about this unusual, but important condition:

> Because of the extremely complex legal and political assessment which must precede any reprisal, it is necessary

76. YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 221 (2004).

77. LAW OF WAR MANUAL, *supra* note 60, § 18.18.2.2, at 1085.

78. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 516.

79. *Id.* at 517.

80. LAW OF WAR MANUAL, *supra* note 60, § 2.4.1.2, at 61.

81. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 518.

82. DINSTEIN, *supra* note 76, at 221.

83. *Id.*

84. *Id.*

85. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 518.

> that the political leadership of a belligerent state decide on any possible use of reprisals. The exact legal nature of the adverse belligerent's actions may be extremely difficult to determine; even more importantly, a decision to use reprisals requires a genuine assessment of the political risks as well as the immediate dangers connected with the use of a reprisal.[86]

The fifth condition is intuitive and consistent with the overarching purpose of reprisals. Under this requirement, reprisal actions must immediately cease as soon as the enemy complies with IHL.[87] This condition is consistent with and highlights the nature of reprisals as a deterrent measure. Finally, the sixth condition prior to using reprisals is that in order to fulfil their purpose, dissuade an adversary from further unlawful conduct, and to promote adherence to IHL, States must announce the action and make it public.[88]

Beyond these six, strictly legal considerations, there are also several practical consequences before resorting to the use of belligerent reprisals. First, resorting to belligerent reprisals may ultimately divert valuable and scarce military resources.[89] Second, since belligerent reprisals are, by definition, violations of international norms, other States may not only disagree with the decision to use them, but also view their use as a violations of IHL and subject to sanction.[90] Third, it is very possible the use of reprisals may strengthen an adversary's morale and will to resist.[91] Fourth, many observers view reprisals as a "race to the bottom," leading to a vicious cycle of counter-reprisals.[92] Finally, like other serious violations of IHL, the use of belligerent reprisals may exacerbate tensions between the parties to the conflict making it more difficult for them to end the armed conflict and return to a peaceful state.[93] Given the legal framework as outlined above, coupled with a number of compelling practical considerations, belligerent reprisals are seemingly a waning IHL enforcement mechanism. Yet, the New Age of Cyber is challenging many seemingly settled areas of international law and therefore it is worth discussing the validity of belligerent reprisals during cyber operations.

86. THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW, *supra* note 36, at 228.

87. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 518.

88. LAW OF WAR MANUAL, *supra* note 60, § 18.18.2.5, at 1086.

89. *Id.* § 18.18.4, at 1090.

90. *Id.*

91. *Id.*

92. *Id.*

93. *Id.*

IV. CYBER OPERATIONS AND BELLIGERENT REPRISALS: THE *LEX LATA*

As a starting point, when thinking about the *lex lata*, it is important to reiterate that the applicable IHL treaties were drafted before cyberspace and operations were a reality.[94] Likewise, there are many challenges associated with the emergence of customary IHL cyber-related norms with the most notable being the highly classified nature of cyber activities by States.[95] However, it is also important to note, as discussed above, it is widely accepted that IHL applies to cyber operations in the context of an armed conflict.[96] With that said, the *Tallinn Manual 2.0* Rules and Commentary provide a valuable resource and assist in identifying issues, gaps, and ambiguities in the law. But, when thinking about the *lex lata*, it is always important to be mindful of whether application of traditional rules of IHL make sense when applied in the cyber context.

This acknowledgment includes the possible use of belligerent reprisals with Rule 108 of *Tallinn Manual 2.0*, which provides basic parameters for use during cyber operations in an international armed conflict. The Rule notes that belligerent reprisals are expressly prohibited against "prisoners of war; interned civilians, civilians in occupied territory or otherwise in the hands of an adverse party to the conflict, and their property; those *hors de combat*; and medical and religious personnel, facilities, vehicles, and equipment."[97] In other circumstances, where international law does not prohibit use "belligerent reprisals are subject to stringent conditions."[98]

The Commentary to Rule 108 provides granularity into the experts' conclusions concerning belligerent reprisals. The experts state, unequivocally, that cyber reprisals are prohibited against the wounded, sick, or shipwrecked; medical personnel, units, establishments, or transports; chaplains; prisoners of war, or interned civilians and civilians in the hands of an adverse party who are protected by the Fourth Geneva Convention, or their property.[99] In effect, these prohibitions are customary international law that binds all States. However, the

94. DINNISS, *supra* note 8, at 239, 241.

95. TALLINN MANUAL 2.0, *supra* note 6, at 377.

96. *Id.* at 3. When one thinks of the use of cyber in the context of an armed conflict, it involves not only the employment of cyber capabilities to objectives in and through cyberspace, but also involves requirements such as weapons reviews to ensure that cyber means of warfare that are acquired or used complies with the law of armed conflict. *Id.* at 375; Michael N. Schmitt & Liis Vihul, *The Emergence of International Legal Norms for Cyberconflict*, *in* BINARY BULLETS: THE ETHICS OF CYBERWARFARE 34, 49 (Fritz Allhoff, Adam Henschke & Bradley Jay Strauser eds., 2016).

97. TALLINN MANUAL 2.0, *supra* note 6, at 460.

98. *Id.*

99. *Id*. at 461.

experts disagreed as to whether customary international law protected cultural property.[100]

Further outlining the proper use of belligerent reprisals in the cyber context, and particularly how AP I's greater prohibitions apply, is Rule 109 of *Tallinn 2.0*. The Rule, rooted in seven different provisions found in AP I, states:

> Additional Protocol I prohibits States Parties from making the civilian population, individual civilians, civilian objects, cultural property and places of worship, objects indispensable to the survival of the civilian population, the natural environment, and dams, dykes, and nuclear electrical generating stations the object of a cyber-attack by the way of reprisal.[101]

The commentary to Rule 109 expands on the general prohibition of cyber reprisals against the aforementioned categories by those States that are parties to AP I and engaged in an international armed conflict.[102] But, the commentary suggests the prohibition is conditional for certain States that adopted understandings during the ratification of AP I.[103] And, despite certain international tribunals holding reprisals against civilians a violation of customary international law, this practice has yet to "crystallise" into a customary rule due to contrary practice.[104] Nevertheless, in substance, the *Tallinn Manual 2.0* experts found that AP I dramatically reduces the use of reprisals in cyber operations by limiting use to only against enemy armed forces, their facilities, and equipment.[105]

Tallinn Manual 2.0's Rule 108, Rule 109, and associated commentary provide an excellent summary of the current law concerning belligerent reprisals in the cyber context. Clearly, the *Tallinn Manual 2.0* agrees that belligerent reprisals have limited use in the contemporary environment as an IHL enforcement mechanism. However, a comparison between belligerent reprisals and the concept of countermeasures under international law may indicate it is time to revisit this determination in the New Age of Cyber. It is important to note that such an intellectual and academic thought experiment, i.e., comparing countermeasures and belligerent reprisals, should not be taken to conflate or confuse these two distinct enforcement mechanisms under international law. They are very different. The common ground between the

100. *Id.* at 463.

101. *Id.*

102. *Id.* at 463–64.

103. *Id.*

104. *Id.* at 464.

105. CORN ET AL., *supra* note 59, at 227. *See generally* KOLB & HYDE, *supra* note 4, at 195.

two is in their underlying purpose and that alone warrants the comparison below.

V. COUNTERMEASURES UNDER INTERNATIONAL LAW

In the first half of the twentieth century, so-called countermeasures were referred to as "peacetime reprisals."[106] Although belligerent reprisals and countermeasures apply under different circumstances, their purpose is fundamentally the same: to force a State that violates international law to discontinue illegal activity.[107] In this respect, countermeasures provide a good point of comparison with belligerent reprisals.

As a threshold matter, it is important to note that States are responsible for their internationally wrongful acts under the law of State responsibility.[108] Article 2 of the International Law Commission's *Articles of State Responsibility for Internationally Wrongful Acts*[109] provides as follows:

> Article 2
> Elements of an internationally wrongful act of a State
>
> There is an internationally wrongful act of a State when conduct consisting of an action or omission:
>
> (a) is attributable to the State under international law; and
> (b) constitutes a breach of an international obligation of the State.[110]

106. Michael N. Schmitt, *Cyber Activities and the Law of Countermeasures*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY 659, 662 (Katharina Ziolkowski ed., 2013). The term peacetime is no longer used.

107. *Id.* at 661–62.

108. *Id.* at 661.

109. Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, (2001), http://www.un.org/law/ilc/ [https://perma.cc/9838-MCGV] [hereinafter Articles on State Responsibility]. Beginning in 1956, the Articles of State Responsibility for Internationally Wrongful Acts were drafted over decades by the International Law Commission. The 59 Articles are divided into four parts: Part One (The Internationally Wrongful Act of the State, articles 1–27); Part Two (Content of the International Responsibility of a State, articles 28–41); Part Three (The Implementation of the International Responsibility of a State, articles 42–54); and Part Four (articles 55–59) contains the final five General Provisions of the text. Although the Articles are not binding, they are authoritative because the International Law Commission developed them over decades under the leadership of multiple special rapporteurs. Schmitt, *supra* note 106, at 661.

110. James Crawford, THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY: INTRODUCTION, TEXT AND COMMENTARIES 81 (2002). As noted in the commentary to Article 2, the element of attribution is sometimes described as "subjective" while the element of a breach is referred to as "objective"; *see* Articles on State Responsibility, *supra* note 109, at 34.

The breach of an international obligation may consist of a violation of a treaty, customary international law, or of general principles of law.[111] For example, internationally wrongful acts may include a cyber operation that violates the sovereignty of another State or the principle of non-intervention among other things. [112] A well-known recent example of an international wrongful act involved the Russian interference in the 2016 U.S. presidential election.[113] According to Professor Michael Schmitt, "Russia's apparent attempt to influence the outcome of the election by its release of emails through WikiLeaks probably violates the international law barring intervention in a state's internal affairs."[114] Another example may be a State that conducts cyber operations against a coastal State from a ship located in the territorial waters of the injured State. These actions would breach international law proscribing innocent passage found in the *United Nations Convention on* the *Law of the Sea*.[115]

One possible consequence for a state that chooses to commit an international wrongful act is entitling a targeted state to resort to countermeasures.[116] "Countermeasures are actions by an injured State that breach obligations owed to the 'responsible' State (the one initially violating its legal obligations) in order to persuade the latter to return to a state of lawfulness."[117] Countermeasures are therefore different than either a retorsion or a plea of necessity. Retorsions are actions taken by a State that are best

111. Articles on State Responsibility, *supra* note 109, at 35.

112. TALLINN MANUAL 2.0, *supra* note 6, at 312–13.

113. *See Russian Hacking and Influence in the U.S. Election*, N.Y. TIMES, https://www.nytimes.com/news-event/russian-election-hacking [https://perma.cc/3FFS-PADV] (last visited Apr. 3, 2018).

114. Ellen Nakashima, *Russia's Apparent Meddling in U.S. Election is Not an Act of War, Cyber Expert Says*, WASH. POST (Feb. 7, 2017), www.washingtonpost.com/news/checkpoint/wp/2017/02/07/russias-apparent-meddling-in-u-s-election-is-not-an-act-of-war-cyber-expert-says/?utm_term=.0e23dfb985de [https://perma.cc/SU9Q-MYGM].

115. Schmitt, *supra* note 106, at 664–65.

116. *See* Int'l Law Comm'n, Rep. on the Work of Its Fifty-Fifth Session, U.N. Doc. A/58/10, at 75 (2003), http://www.un.org/law/ilc/ [https://perma.cc/57YV-NKTX] [hereinafter Articles on State Responsibility II] ("The wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State in accordance with chapter II of Part Three.").

117. Michael Schmitt, *International Law and Cyber Attacks: Sony v. North Korea*, JUST SECURITY (Dec. 17, 2014), http://justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/ [https://perma.cc/CN2H-5JRZ]; *see also* TALLINN MANUAL 2.0, *supra* note 6, at 111 (describing countermeasures as "actions or omissions by an injured State [in response to internationally wrongful acts] directed against a responsible State that would violate an obligation owed by the former to the latter.").

described as unfriendly, but not inconsistent with an international obligation of a State.[118] An example includes limitations upon normal diplomatic relations or other contacts, embargos of various kinds, or withdrawal of voluntary aid programs.[119] A plea of necessity, on the other hand, denotes exceptional cases where a State, faced with grave and imminent peril to an essential interest, takes measures counter to its international obligations to safeguard those particular interests.[120] In the cyber context, an example of the circumstances leading to a plea of necessity may involve a cyber operation against a State's critical infrastructure.[121] In contrast to either a retorsion or a plea of necessity, a countermeasure allows "a state victimized by another . . . to use acts traditionally prohibited under international law to force the offending state to comply with their legal obligations."[122]

In describing countermeasures in a cyber context, Professor William Banks commented that "[c]ountermeasures are responses, whether cyber in nature or not, below the use of force threshold designed to prevent or mitigate a perpetrator State from continuing its unlawful cyber intervention."[123] In this regard, countermeasures are similar to belligerent reprisals in that they allow a State to act unlawfully in order to force international legal compliance.[124] Of course there are differences between the two—countermeasures only apply below the use of force threshold, are limited in severity,[125] and must not involve the threat or use of force[126]—whereas belligerent reprisals only apply during an international armed conflict and would otherwise violate IHL but for a prior illegal act.[127] Nevertheless, despite these differences, countermeasures provide

118. Schmitt, *supra* note 117.

119. *Id.*

120. DINNISS, *supra* note 8, at 102.

121. Schmitt, *supra* note 106, at 663.

122. Daniel Garrie & Shane R. Reeves, *So You're Telling Me There's a Chance: How the* Articles on State Responsibility *Could Empower Corporate Responses to State-Sponsored Cyber Attacks*, HARV. NAT'L SECURITY J. ONLINE FEATURES 5 (2015), http://harvardnsj.org/wp-content/uploads/2016/01/Garrie-and-Reeves-Non-State-Actor-and-Self-Defense.pdf [https://perma.cc/SY6X-W7PR].

123. William Banks, *State Responsibility and Attribution of Cyber Intrusions After* Tallinn 2.0, 95 TEX. L. REV. 1487, 1501 (2017).

124. Schmitt, *supra* note 106, at 662. As noted by Professor Schmitt, the idea of a reprisal was also thought of in a *jus ad bellum* context. That is, "[t]he historical notion of reprisals was broader than that of countermeasures in that it included both non-forceful and forceful actions. Today, forceful reprisals have been subsumed into the U.N. Charter's use of force paradigm, which allows States to resort to force in response to armed attacks." *Id.*

125. Articles on State Responsibility II, *supra* note 116, at 129.

126. *Id.* at 131. *See generally* TALLINN MANUAL 2.0, *supra* note 6, at 38.

127. Schmitt, *supra* note 106, at 662.

a valuable lens by which to view belligerent reprisals in the context of cyber operations. Accordingly, there are four features of countermeasures worth highlighting: (1) the purpose of countermeasures; (2) restrictions or limitations on their use; (3) proportionality; and (4) attribution standards.

The purpose of a countermeasure is to return a situation to a condition of lawfulness[128] by inducing a State, who is responsible for internationally wrongful acts, to comply with its obligations and where appropriate make assurances or guarantees and reparations. Rule 21 of *Tallinn Manual 2.0* further speaks to the purpose of countermeasures in the context of cyber. It provides that "[c]ountermeasures, whether cyber in nature or not, may only be taken to induce a responsible State to comply with the legal obligations it owes an injured State."[129] Furthermore, by definition, countermeasures are a reactive, remedial, self-help measure necessitated by a lack of a compulsory dispute resolution mechanism, and are a product of a decentralized system by which an aggrieved State may seek to vindicate its rights and restore a proper legal relationship with the responsible State.[130]

It is important to note, however, that countermeasures are not intended as punishment.[131] Yet, like other forms of self-help, countermeasures are subject to abuse, especially between States of unequal power.[132] And, similar to belligerent reprisals, it may be difficult to distinguish the precise motive for pursuing the countermeasure. In other words, a pertinent question is whether countermeasures exacted against a State are being done to induce the State, who is responsible for internationally wrongful acts, to comply, or is it being done in retaliation, retribution, or revenge? In answering this question, if the countermeasure will only exacerbate a situation, it is likely a fair indication the motive may be rooted more in retaliation.[133]

The second inquiry involves restrictions on the use of countermeasures. The most significant restriction stems from the use of force as proscribed by

128. *Id.* at 674.

129. TALLINN MANUAL 2.0, *supra* note 6, at 116. Speaking to the underlying mind set of countermeasures "should be a wager on the wisdom, not on the weakness of the other Party. They should be used with a spirit of great moderation and be accompanied by a genuine effort at resolving the dispute." *Case Concerning the Air Service Agreement of 27 March 1946 Between the United States of America and France*, 18 U.N. REP. INT'L ARBITRAL AWARDS 417, 445. One particular risk in the context of cyber is the speed at which cyber operations may unfold, both intentionally wrongful acts and countermeasures, may detract from careful consideration of intent and consequences.

130. Schmitt, *supra* note 106, at 662; DINNISS, *supra* note 8, at 281.

131. Schmitt, *supra* note 106, at 674.

132. *Id.*

133. TALLINN MANUAL 2.0, *supra* note 6, at 117.

Article 2(4) of the United Nations Charter.[134] Articles 49 and 50 of the *Articles of State Responsibility for Internationally Wrongful Acts* further define the limits of the legal boundaries on the use of countermeasures.[135] Under Article 49, constraints exist on a countermeasure's object and purpose and are limited to the responsible State's period of non-performance of its international obligations.[136] Additionally, as far as possible, countermeasures must be taken in such a way to permit the resumption of performance of the obligation in question.[137] Article 50 expands on the foregoing by specifying a number of international obligations the performance of which may not be impaired by countermeasures.[138] Drawing from Article 50, *Tallinn Manual 2.0*, Rule 22 provides that "[c]ountermeasures, whether cyber in nature or not, may not include actions that affect fundamental human rights, amount to prohibited belligerent reprisals, or violate peremptory norm. A State taking countermeasures must fulfil its obligations with respect to diplomatic and consular inviolability."[139]

The third inquiry when considering the use of countermeasures involves the notion of proportionality.[140] Article 51 of the *Articles of State Responsibility* provides that "[c]ountermeasures must be commensurate with the injury[141] suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[142] Much like the "purpose" of countermeasures,

134. U.N. Charter art. 2, ¶ 4. This provision also reflects customary international law. As noted by Professor Schmitt, the dilemma lies in determining when a cyber operation qualifies as a use of force thereby making it impermissible as a countermeasure. *See* Schmitt, *supra* note 106, at 678.

135. Articles on State Responsibility II, *supra* note 116, at 129–34.

136. *Id.* at 129.

137. *Id.*

138. *Id.* at 131.

139. TALLINN MANUAL 2.0, *supra* note 6, at 122–23.

140. It is important to note that proportionality with respect to countermeasures is separate and distinct from the concept of proportionality in *jus ad bellum* or IHL. With respect to *jus ad bellum*, the concept of proportionality considers the degree of force necessary for a State to defend itself against an armed attack. In that context, proportionality serves to identify the circumstances in which the unilateral use of force is permissible under international law. Additionally, it also serves to determine the intensity and the magnitude of military operations. In the context of IHL, proportionality means essentially whether an attack shall be cancelled or suspended if the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof. *See* Protocol I, *supra* note 13, art. 51, at 37, art. 57, at 41–42.

141. Articles of State Responsibility II, *supra* note 116, at 134. "Injury" means a breach of an international legal obligation. It should not be understood to require damage. *See* TALLINN MANUAL 2.0, *supra* note 6, at 127.

142. Articles of State Responsibility II, *supra* note 116, at 134; DINNISS, *supra* note 8, at 103–04. The principle of proportionality is a deeply rooted requirement for countermeasures and is widely recognized in State practice, doctrine and international jurisprudence. For example, in the *Naulilaa* case, using the word "reprisal," the court stated, "Even if one admitted that international law does not

proportionality is also an essential limitation on the injured State in terms of the employment of specific countermeasures and the level of their intensity.[143] A countermeasure that is disproportionate amounts to an impermissible punishment or retaliation, and is contrary to the object and purpose of countermeasures.[144] A proportionality analysis provides a check on the potentially escalating effect of countermeasures and is a control on the exercise of "decentralized power conferred on States to react individually to international wrongful acts."[145] However, it is important to note that proportionality does not mean or imply reciprocity.[146] In fact, it is entirely lawful to use non-cyber countermeasures in responses to an internationally wrongful act involving cyber operations.[147]

In the context of cyber, it is feasible to narrowly tailor the intensity, duration, and effects of the operation. For example, a cyber operation aimed at incapacitating infrastructure without destroying it may be particularly useful in meeting the limitations on countermeasures, including proportionality.[148] Noting the challenges of assessing proportionality in the context of countermeasures, *Tallinn Manual 2.0* states, in part:

> The interconnected and interdependent nature of cyber systems can render it difficult to determine accurately the consequences likely to result from cyber countermeasures. States must therefore exercise considerable care when assessing whether their countermeasures will be proportionate. Conducting a full assessment may require, for instance, mapping the targeted system or reviewing relevant intelligence. Whether the assessment is adequate depends on the foreseeability of potential consequences and the feasibility of means that can be used to conduct it.[149]

The final issue with respect to countermeasures concerns attribution. The issue of attribution includes more than technically determining the source of the

require that the reprisal be approximately measured by the offense, one should certainly consider as excessive, and thus illegal, reprisals out of all proportion with the act which motivated them." Naulilaa Incident Arbitration, Portuguese-German Arbitral Tribunal, 1928, *reprinted and translated in* WILLIAM W. BISHOP, JR., INTERNATIONAL LAW: CASES AND MATERIALS 903, 904 (3d ed. 1971).

143. DINNISS, *supra* note 8, at 104.

144. TALLINN MANUAL 2.0, *supra* note 6, at 127.

145. JAMES CRAWFORD, STATE RESPONSIBILITY: THE GENERAL PART 698 (James Crawford & John S. Bell eds., 2013).

146. *See* DINNISS, *supra* note 8, at 104.

147. TALLINN MANUAL 2.0, *supra* note 6, at 128.

148. MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 106 (2014).

149. TALLINN MANUAL 2.0, *supra* note 6, at 128.

attack. It also includes policy and legal issues. The difficulties in attributing cyber-attacks and determining the identity of the perpetrators causes a perception that States can operate with virtual impunity in the cyber realm.[150] The various tools, tactics, and techniques available to conceal cyber activities compounds the challenges to attribute attacks to States, non-State actors, or individuals.[151] For example, a responsible State may gain "control of another State's cyber infrastructure and use it to mount harmful" attacks against a third State.[152] This situation illustrates the technical complexities that exist in the cyber domain. While future technological innovations may mitigate the attribution obstacle, "as with any forensic investigation, information gathering" in cyberspace is likely to remain technically challenging, time consuming, and resource intensive.[153]

While ascertaining the source of a cyber-attack remains problematic, some influential thought leaders have challenged the paradigmatic thinking that discovering the point of attack and those individuals responsible is necessary for the purpose of attribution.[154] Proponents of this concept disagree that once the technical forensics of the attack is established only then can attribution hope to determine the person or organization responsible for it.[155] Instead, they conceptualize the problem of attribution as one to consider in the light of this question: What do national policy leaders actually need to know about the cyber operation?[156] In answering this question, national leaders should simply know who is ultimately responsible for the attack rather than who actually committed the acts.

An example of this distinction between determining responsibility versus identifying the actual perpetrators occurred in 1999 when NATO inadvertently bombed the Chinese embassy in Belgrade during the armed conflict in Kosovo.[157] In the aftermath of the tragedy, scores of people gathered in Beijing near the U.S. Embassy, including many students bused in for the protests.[158]

150. Michael N. Schmitt & Liis Vihul, *Proxy Wars in Cyberspace: The Evolving International Law of Attribution*, FLETCHER SECURITY REV., Spring 2014, at 53, 54 (2014).

151. Schmitt, *supra* note 106, at 685.

152. *Id.*

153. Louise Arimatsu, *Classifying Cyber Warfare*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 326, 333 (Nicholas Tsagourias & Russell Buchan eds., 2015).

154. Jason Healy, *The Spectrum of National Responsibility for Cyberattacks*, BROWN J. WORLD AFF., Fall/Winter 2011, at 57, 57 (2011).

155. *Id.*

156. *Id.*

157. *Id.* at 58.

158. *Id.*

Despite protesters pummeling the U.S. Embassy with bricks and rocks,[159] U.S. authorities did not seek to identify the individual stone throwers "because the exact attribution was not an important input for decision makers."[160] The United States knew that the Chinese were responsible for attacks regardless of who threw the individual rocks.[161] Even though knowing who actually threw the rocks would provide many data points, that information would not be particularly helpful to deciding how to respond to the incident.[162] Similarly, with cyber-attacks, it is often not necessarily probative who actually initiated the attack at the lowest technical level.[163] Instead, the most important determination is who is overall responsible. In sum, reconceptualizing the concept of attribution may serve to provide decision-makers with flexibility to respond in the complex domain of cyber.[164]

Countermeasures have become an important tool, even if not used, for States to force compliance with international law in cyber space below the use of force threshold.[165] Taking the foregoing background into consideration, countermeasures are, in many respects, the other side of the belligerent reprisal coin. It is therefore worth asking whether belligerent reprisals may serve an equally useful purpose as countermeasures when addressing cyber operations in the international armed conflict context.

159. *Chinese in Belgrade, Beijing Protest NATO Embassy Bombing*, CNN (May 9, 1999, 9:44 PM), http://edition.cnn.com/WORLD/asiapcf/9905/09/china.protest.03/ [https://perma.cc/E6EG-QQZF].

160. Healy, *supra* note 154, at 58.

161. *Id.*

162. *Id.*

163. *Id.* at 57.

164. Attribution also presents challenging legal and factual issues. For example, what are the evidentiary considerations when using countermeasures? The Commentary to the *Articles on State Responsibility* suggest the standard for factual attribution is identification with responsible certainty, *see* Schmitt, *supra* note 106, at 685, and, importantly, only States may use countermeasures. TALLINN MANUAL 2.0, *supra* note 6, at 130. This restriction thus precludes private firms, like Sony for instance, from engaging in "hack-back" countermeasures against North Korea after a cyber-attack in 2014. *See generally* David E. Sanger, David D. Kirkpatrick & Nicole Perlroth, *The World Once Laughed at North Korean Cyberpower. No More.*, N.Y. TIMES (Oct. 15, 2017), https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html [https://perma.cc/985U-TXV8]. *But see generally* Garrie & Reeves, *supra* note 122, at 13 (discussing a possible way for a corporation to use countermeasures).

165. *See, e.g.*, Nakashima, *supra* note 114 (noting that the United States most likely has grounds to use countermeasures against Russia for the 2016 election hacking actions) (quoting Professor Michael Schmitt).

VI. BELLIGERENT REPRISALS AND CYBER: A THEORETICAL FRAMEWORK

Sir Hersch Lauterpacht, one of the leading international lawyers of the twentieth century, observed that "[i]f international law is, in some ways, at the vanishing point of law, the law of war is, perhaps even more conspicuously, at the vanishing point of international law."[166] At some level, Lauterpacht's insightful remarks are not surprising in that IHL is attempting to regulate the worst of human conditions—war. International Humanitarian Law seeks to introduce moderation and restraint into a pursuit defined by violence and death, unbridled passion and hatred, as well as confusion and unpredictability. At its best, IHL is never more than imperfectly observed, and at its worst, very poorly observed.[167] Commenting on the effectiveness of the *jus in bello*, distinguished British historian Geoffrey Best stated, "[w]e should perhaps not so much complain that the law of war does not work well, as marvel that it works at all."[168] Unquestionably, Best is absolutely correct in his assessment. Yet, beyond the substance and circumstances of what IHL attempts to regulate, there is another factor that places international law generally, and IHL specifically, at the "vanishing point of law"—anemic enforcement mechanisms.

The challenges in enforcing and implementing norms are a significant reason why international law faces enduring criticism. Arguably, meaningful enforcement is the Achilles heel of this area of law, especially if "law" is the commands of a sovereign backed by sanctions as articulated by legal positivists from Hobbes to Austin.[169] Furthermore, critics have long contended the intractable problem of meaningful enforcement and sanctions in international law not only undermines the effectiveness and credibility of the international normative system, but also suggests whether international law is "law" at all if it cannot be imposed.[170] Even then, one has to be careful not to overstate the problem and place international law in the proper context:

> The international situation cannot be equated to the situation within states. There is not a powerful international body that has authority over the subjects of the law; the international community does not have an international police force and a

166. BEST, *supra* note 11, at 12.

167. *Id.* at 11.

168. *Id.* at 12.

169. Jack Goldsmith & Daryl Levinson, *Law for States: International Law, Constitutional Law, Public Law*, 122 HARV. L. REV. 1791, 1822 (2009).

170. Elena Katselli Proukaki, *The Problem of Enforcement in International Law: Countermeasures, the Non-Injured State and the Idea of International Community*, INT'L L. OBSERVER (May 18, 2010, 11:23 AM), http://www.internationallawobserver.eu/2010/05/18/the-problem-of-enforcement-in-international-law-countermeasures-the-non-injured-state-and-the-idea-of-international-community [https://perma.cc/S9UZ-6EW6].

> judiciary with compulsory jurisdiction; thus, coercive power exercised by the international community cannot be relied upon to enforce international obligations. The sovereignty and equality of states precludes the operation of such mechanisms, and ensures that the execution of the law is precarious and, sometimes, irregular.[171]

Although difficulties exist in enforcing IHL, there are some mechanisms for enforcement including protecting powers,[172] fact finding commissions,[173] penal sanctions,[174] and reparations.[175] But, challenges still remain. The absence of a hierarchical system or institution capable of enforcement, implementation, and accountability fundamentally precludes IHL's decentralized character from undergoing meaningful change in the foreseeable future. So, how should the international community respond when confronted with the realities of international law? Do advances in technology provide an opportunity to better promote lawfulness on the modern battlefield? In the context of cyber and the emergence of new capabilities, revisiting belligerent reprisals provides a means to overcome the obvious challenges underlying the enforcement of IHL.

One way to conceptualize or consider the issue of belligerent reprisals is to think of them as three points on a left-to-right continuum. At the far left end of the continuum, the first category, are belligerent reprisals that should never

171. KOLB & HYDE, *supra* note 4, at 283.

172. Under IHL, a "protecting power" is a neutral, third-party State designated as a party to the conflict and accepted by the enemy party. This State has agreed to carry out the functions assigned to a protecting Power under IHL. These functions include monitoring and ensure compliance with the law. In the absence of an agreement, the ICRC or any other impartial humanitarian organization may designate a protecting power substitute. Notably, the use of this system is rare in recent years. *See Protecting Powers: How Does the Law Protect in War?*, INT'L COMM. RED CROSS, https://casebook.icrc.org/glossary/protecting-powers [https://perma.cc/CZ47-2G5G] (last visited Jan. 26, 2018).

173. Article 90 of the 1977 Additional Protocol I provides for the establishment of an International Fact-Finding Commission. Established in 1991, it is a permanent body of 15 independent experts acting in their personal capacity. The Commission's purpose is to contribute to implementation of and ensure respect for IHL in armed conflicts. Thilo Marauhn, *The International Humanitarian Fact Finding Commission—Dedicated to Facilitating Respect for International Humanitarian Law*, INT'L HUMANITARIAN FACT-FINDING COMM'N, www.ihffc.org/index.asp?Language=EN&page=home [https://perma.cc/8YXN-9DHV] (last visited Jan. 26, 2018).

174. International Humanitarian Law is enforceable in both domestic courts and international tribunals. Over the last three decades there has been significant efforts internationally to prosecute war crimes in ad hoc tribunals like the International Criminal Tribunals for the former Yugoslavia and Rwanda as well as the International Criminal Court.

175. HUMA HAIDER, GSDRC, INTERNATIONAL LEGAL FRAMEWORKS FOR HUMANITARIAN ACTION: TOPIC GUIDE 49 (2013), http://www.gsdrc.org/topic-guides/international-legal-frameworks-for-humanitarian-action/challenges/compliance-with-and-enforcement-of-ihl/ [https://perma.cc/FF3Z-XKFX].

occur regardless of the motive, means, or method. For example, belligerent reprisals against persons under the control of a party to the conflict should never be the target of a reprisal. As a representative list, this would include the following category of individuals: "prisoners of war; interned civilians, civilians in occupied territory or otherwise in the hands of an adverse party to the conflict, and their property; those *hors de combat*; and medical and religious personnel, facilities, vehicles, and equipment."[176]

This first category also contains certain objects immune as targets of reprisals, including medical buildings, vessels, or equipment; works or installations containing dangerous forces; objects indispensable to the survival of the civilian population; and cultural property and places of worship.[177] Furthermore, the belligerent reprisals continuum precludes the use of chemical or biological weapons.[178] Certain cyber operations that would fit into the above category include opening the flood gates of a dam causing the release of a body of water capable of widespread destruction; or, using a cyber-attack to target a hospital by turning off its electricity or taking some action to remotely taint the food or water supply for the civilian population.

There are a number of reasons to categorically exclude the foregoing belligerent reprisals. First, attacking these persons and objects are simply too inhumane and barbaric. If IHL seeks to balance between the meta-principles of military necessity and humanity, the above egregious and irreversible acts may never been offset by necessity. The second reason goes to the underlying purpose of belligerent reprisals, i.e., to induce an adversary to comply with IHL. The above examples will likely cause an escalation in violence by inflaming passions and resentments, leading additional violations of IHL and continued hostilities. Third, using countermeasures as an analogy, these actions are neither reversible nor likely to induce a return to lawfulness. Instead, the harshness of the acts make them more analogues to punishments and retaliation, and whether exacted in the cyber realm or not, these belligerent reprisals should be categorically banned.

At the far right end of the continuum are belligerent reprisals that do not shock the conscience and, in the gritty world of pragmatism, are reasonable and rational responses to induce an adversary's compliance with IHL.[179] To some that take an absolutist approach to reprisals, the suggestion that there is any place on the continuum for belligerent reprisals is cause for great concern. But,

176. TALLINN MANUAL 2.0, *supra* note 6, at 460.

177. Mitchell, *supra* note 50, at 162–64.

178. LAW OF WAR MANUAL, *supra* note 60, § 18.18.3.4, at 1088.

179. Michael A. Newton, *Reconsidering Reprisals*, 20 DUKE J. COMP. & INT'L L. 361, 361 (2010).

even the ICRC in their 2005 *Study on Customary International Humanitarian Law* did not take the position that there is a complete ban on belligerent reprisals.[180] Rule 145 of the *Study* stated, "Where not prohibited by international law, belligerent reprisals are subject to stringent conditions."[181]

An example at this end of the spectrum may involve the use of a prohibited weapon against combatants or military objectives.[182] For example, suppose a State is a party to the Convention on Cluster Munitions[183] or Ottawa Convention[184] and uses cluster munitions or antipersonnel mines as a belligerent reprisal against another State party. Assuming, *arguendo*, that the other criteria for a belligerent reprisal are met, such an action is permissible.[185] For somewhat obvious reasons, the parallel to countermeasures would be the strongest in this type of case.

Tallinn Manual 2.0 provides a hypothetical to illustrate a lawful cyber operation for those States not a party to 1977 AP I.[186] In the scenario, the armed forces of one State bomb the medical facilities of another State in the context of an armed conflict and the victim State is not a party to AP I.[187] In response, and after repeated demands to cease the bombings, the Prime Minister of the victim State approves a cyber-attack against a power generation facility used exclusively to provide power to the civilian population.[188] The purpose of this cyber reprisal operation is to compel the State which was attacking the medical facilities to stop.[189] So long as the Prime Minister orders the cessation of cyber-attacks as soon as the aggressive state stops attacking its medical facilities, the reprisal is legal according to the *Tallinn Manual 2.0* experts.[190]

The middle of the continuum is the most important to this analysis and one where the employment of cyber means and methods are legitimate so long as their purpose is to induce an adversary to be in compliance with IHL and so long as they are tailored to mitigate some of negative and collateral effects. It

180. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 513.

181. *Id.*

182. WILLIAM H. BOOTHBY, WEAPONS AND THE LAW OF ARMED CONFLICT 54 (2009).

183. THE CONVENTION ON CLUSTER MUNITIONS, www.clusterconvention.org/ [https://perma.cc/FM5T-XBZ4] (last visited Oct. 21, 2018).

184. *Anti-Personnel Landmines Convention*, UNITED NATIONS OFF. GENEVA, www.un.org/disarmament/geneva/aplc/ [https://perma.cc/G3M3-AWNE] (last visited Oct. 21, 2018).

185. BOOTHBY, *supra* note 182, at 54.

186. TALLINN MANUAL 2.0, *supra* note 6, at 462.

187. *Id.*

188. *Id.*

189. *Id.*

190. *Id.* The Experts did note that if the belligerent reprisal involved attacking the other State's medical facilities that would be considered unlawful under *Tallinn Manual 2.0*, Rule 108.

is important to reiterate that the ability to develop and execute belligerent reprisals in the middle of the continuum depends, in part, on whether the State is a party to AP I as seen in the example above. The United States, again, is not a party to AP I with one of the primary reasons being the wide-ranging prohibitions against reprisals.[191] The United States' position in this case stemmed from its concern about what could lawfully be done immediately to stop an enemy State from violating IHL.[192]

So, what are the likely objects a State may attack as a belligerent reprisal that would be considered in the middle of the continuum? So long as a State meets all the criteria as outlined above in Part III,[193] reprisals may include a cyber operation against a portion of a State's economic infrastructure such as communication and transportation networks, financial markets, or energy sectors.[194] These reprisals would need to be narrowly tailored such that they cause disruption, inconvenience or, in some cases, perhaps reversible non-permanent damage to a target.[195] Additionally, using a reprisal to target the civilian leadership of a State in order to exploit damaging personal and professional information may induce a State adversary to comply with IHL. This is a non-exhaustive list of potential targets for a cyber reprisal and are best viewed as illustrating the middle of the continuum. However, what becomes apparent is that through the use of cyber belligerent reprisals a State can meaningfully enforce IHL compliance without causing repugnant and irreparable harm. Of course, further discussion on the reconceptualization of cyber belligerent reprisals is necessary to provide greater clarity on the middle of the continuum.

Viewing cyber reprisals along this continuum provides decision-makers the flexibility of options to respond in a lawful manner against a belligerent State while also remedying the shortcoming of enforcing IHL. While belligerent reprisals have been generally discarded by the international community, and justifiably so, cyber operations warrant a re-examination of this tool for IHL enforcement. A dialogue between States on this possibility would be a worthy endeavor.

VII. CONCLUSION

In sum, the employment of belligerent reprisals is a course of action with wide-ranging implications and should never be undertaken lightly.

191. Matheson, *supra* note 59, at 420.

192. SOLIS, *supra* note 10, at 132.

193. *See supra* notes 66–93 and accompanying text.

194. ROSCINI, *supra* note 148, at 104.

195. *Id.* at 106.

Nevertheless, they are lawful acts if approved at the highest levels of government with the purpose to compel an adversary to comply with IHL. Using this ancient enforcement mechanism provides a means to overcome the anemic deficiency of enforcing IHL. Although there have been efforts to impose meaningful international penal sanctions in the past few decades, much more needs to be done *during* the armed conflict itself to ensure compliance. As illustrated in this article, cyber means and methods create opportunities to compel an adversary to comply with IHL while, at the same time, mitigating the effects of cyber operations.

Some well-intentioned individuals and groups may summarily dismiss belligerent reprisals because of the horrific abuses and risks associated with their use. But, viewing countermeasures as a conceptual backdrop in terms of purpose and limitations, the time has come to at least consider the possibilities at the intersection of IHL and emerging technologies. As uncivilized, repugnant, and archaic as it may seem, strictly controlled reprisals may be justifiable as a proportionate response to the criminal acts committed by an adversary to prompt compliance with the law. Emerging cyber means and methods may be the right tool at the right time to do just that.