Give Them an Inch, They'll Take a Terabyte: How States May Interpret *Tallinn Manual 2.0*'s International Human Rights Law Chapter

Robert E. Barnsby and Shane R. Reeves*

> The development of norms for [S]tate conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding [S]tate behavior—in times of peace and conflict—also apply in cyberspace.[1]

Introduction

The recent publication of *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, the "follow-on initiative [expanding *Tallinn Manual 1.0*'s] scope to include the public international law governing cyber operations during peacetime,"[2] is a truly remarkable accomplishment in both cyber and international law. Unquestionably, it is the most comprehensive work ever written to describe how international law regulates cyber activities that take place below the use-of-force threshold. As this Article underscores, the significance of the *Manual*'s publication is further enhanced by its Chapter seeking to "articulate[] Rules indicating the scope of application and content of international human rights law [(IHRL)] bearing on cyber activities."[3]

---

* Robert E. Barnsby is an Assistant Professor of Law at West Point and the Army Cyber Institute's Cyber Law Fellow. Shane R. Reeves is an Associate Professor and Deputy Head of the Department of Law at West Point and a Lieutenant Colonel in the United States Army. The views expressed here are their personal views and do not necessarily reflect those of the Department of Defense, the United States Army, the United States Military Academy at West Point, or any other department or agency of the United States Government. The analysis presented here stems from their academic research of publicly available sources, not from protected operational information. This article refers throughout its text to States (capitalized when used in accordance with the Westphalian / International Humanitarian Law (IHL) nation-state concept), Internet (capitalized), and cyberspace (one word), all consistent with the *Tallinn Manual*'s usage of those same terms.

1. WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [https://perma.cc/49T9-QUER].

2. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 1 (Michael Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0].

3. *Id.* at 179.

An international group of "scholars and practitioners with expertise in the legal regimes implicated by peacetime cyber activities"[4] (International Group of Experts) authored the *Manual* (*Tallinn 2.0*) between 2013 and 2016 over the course of a series of formal meetings and workshops held in Tallinn, Estonia.[5] Like the *Manual* itself, it is inevitable that the *Manual*'s IHRL Chapter will be studied and debated endlessly. Less concerned with this overall debate than with the need for practitioners to understand specific assertions made within the human rights Chapter, this Article closely examines certain key terms in the text to ascertain their impact on daily cyber activities at the State (national) level. A granular view of the IHRL Chapter reveals these key terms to be often vague and ill-defined, resulting in definitional gaps capable of being used by States to undermine IHRL progress over time.

After background discussion laying the foundation for IHRL and identifying the actual human rights contemplated by the International Group of Experts in the IHRL Chapter (Part II), this Article identifies several important yet undefined terms and concepts throughout the work. Part III centers on perhaps the most significant example of an undefined concept, "countering terrorism,"[6] which the Experts state without further explanation to be a "legitimate purpose" allowing States to monitor online communications without violating the right to privacy.[7] While the International Group of Experts offers checks on possible abuse, this section demonstrates the challenges of constraining a State intent on using the "countering terrorism" exception to swallow the rule requiring States to respect and protect international human rights.[8] Even key terms such as the

4. *Id.* at 1.

5. *Id.* at 5–6. Tallinn, Estonia has embraced its status as home to NATO's Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), "a renowned research and training institution," *id.* at 1, virtually ever since "Estonia suffered massive cyber attacks, primarily from ethnic Russian non-state actors" in 2007. Michael N. Schmitt, *The Law of Cyber Warfare:* Quo Vadis*?*, 25 STAN. L. & POL'Y REV. 269, 269 (2014).

6. TALLINN MANUAL 2.0, *supra* note 2, at 203.

7. *Id.*

8. The International Group of Experts identifies five rules that form the basis of IHRL's bearing on cyber activities. Rule 34 states that IHRL is "applicable to cyber-related activities." *Id.* at 182. Rule 35 states that "[i]ndividuals enjoy the same international human rights with respect to cyber-related activities that they otherwise enjoy." *Id.* at 187. Rule 36 outlines "[o]bligations to respect and protect international human rights," as further elucidated throughout the text of this Article. *Id.* at 196. Rule 37 reminds the reader that "[t]he obligations to respect and protect international human rights . . . remain subject to certain limitations that are necessary to achieve a legitimate purpose," as discussed throughout this Article. *Id.* at 201–02. Rule 38 contemplates "[a State's ability to] derogate from its human rights treaty obligations . . . when permitted, and under the conditions established, by the treaty in question." *Id.* at 207.

word "terrorism" are nebulous to the reader and exemplify the ambiguity on which a State may rely to limit human rights.[9]

Part IV analogizes the gaps in *2.0* to a similarly critical, unforeseen gap in *Tallinn 1.0* (above the use-of-force-threshold activities) to illustrate how both manuals similarly act as a general framework for application of international law to cyber activities while leaving specifics to be filled in by State practice. Although the International Group of Experts is not optimistic there will be more than a paucity of State practice[10] available due to secrecy challenges, and provides another vague term suggesting "effective measures"[11] will be allowed, this Article suggests there are examples of unclassified, ongoing State practices that both help define the vague "effective measures" term and indicate the ability to overcome the secrecy challenge in this area. Unclassified U.S. cyber programs designed to gather intelligence, map networks, and prepare for military operations against an adversary in the cyber realm are described here in an effort to illustrate the (perhaps) overstated secrecy concerns.[12] Finally, mindful that "[m]any commentators assert customary international law as they would like it to be, rather than as it actually is,"[13] this Article does not suggest any particular State practice has risen to the level of customary international law in these areas. Nevertheless, the aspects of State practice described *infra* amplify our understanding of what the IHRL Chapter seeks to achieve with its admirable efforts to codify online rights "in accordance with international human rights law."[14]

I. Background

The United Nations Charter lays the foundation for international human rights law. While primarily a *jus ad bellum* instrument, the purposes and principles of the charter recognize the need for human rights and "for fundamental freedoms for all without distinction as to race, sex, language, or religion."[15] This statement ensures the protection of persons as individuals "rather than as subjects of sovereign States" and imposes certain legal

9. *See infra* notes 37–45 and accompanying text.

10. *See infra* note 74 and accompanying text.

11. TALLINN MANUAL 2.0, *supra* note 2, at 199.

12. *See infra* notes 85–87 and accompanying text.

13. John B. Bellinger, Legal Advisor, U.S. Dep't of State, Lecture by Mr. Bellinger for Oxford Leverhulme Programme on the Changing Character of War (Dec. 10, 2007), https://2001-2009.state.gove/s/l/2007/112723.htm [https://perma.cc/V9PJ-XCNC].

14. TALLINN MANUAL 2.0, *supra* note 2, at 179.

15. U.N. Charter art. 1, ¶ 3; *see also* Brian J. Bill, *Human Rights: Time for Greater Judge Advocate Understanding*, ARMY LAW., June 2010, at 54, 54–55 (discussing cursorily the United States' role in the development of international human rights law).

requirements on State actors.[16] Composed of both treaty[17] and customary obligations, this body of international law, as noted throughout the *Tallinn Manual 2.0* IHRL Chapter, applies in cyberspace.[18]

While no definitive list of human rights in cyberspace exists,[19] certain rights are especially relevant in the cyber context. The International Group of Experts provides a nonexhaustive list of particularly important human rights applicable in cyberspace, including freedom of expression, freedom of opinion, due process, and perhaps most importantly, privacy.[20] Rule 35 of the IHRL Chapter notes the central importance of privacy in cyberspace but also cautions that the precise scope of the right is unsettled.[21] Further, the International Group of Experts acknowledges the view that the right to privacy has "not yet crystallized into a customary norm."[22] Yet, despite these caveats, a reading of the *Manual* makes clear that an individual's right to privacy in cyberspace, similar to other international human rights,[23] is to be respected and protected by State actors.[24]

Furthermore, although certain fundamental human rights are considered nonderogable,[25] such as the prohibition on slavery, the prohibition on torture,

---

16. RICHARD P. DIMEGLIO ET AL., U.S. ARMY JUDGE ADVOCATE GEN.'S LEGAL CTR. & SCH., INT'L & OPERATIONAL LAW DEP'T, LAW OF ARMED CONFLICT DESKBOOK 195 (William J. Johnson & Andrew D. Gillman eds., 2012) [hereinafter DESKBOOK].

17. *See, e.g.*, International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171 (committing its State signatories to protection of the civil and political rights of individuals).

18. Specifically, Rule 34 states that "[i]nternational human rights law is applicable to cyber-related activities." TALLINN MANUAL 2.0, *supra* note 2, at 182. Rule 35 states that "[i]ndividuals enjoy the same international human rights with respect to cyber-related activities that they otherwise enjoy." *Id.* at 187. The International Group of Experts "agreed that both treaty and customary international human rights law apply to cyber-related activities, [though] they cautioned that it is often unclear as to whether certain human rights reflected in treaty law have crystallised as rules of customary law." *Id.* at 179. Making clear that "States may, under specific circumstances . . . , limit the exercise and enjoyment of certain rights," *id.*, this entire Chapter in *Tallinn 2.0* is reflective of the ability to limit States' "obligations to respect and protect international human rights." *Id.* at 201 (Rule 37). While ostensibly necessary to circumscribe nonabsolute (or fundamental) rights, the Group of Experts' empowerment of States' abilities to define for themselves what is "necessary to achieve a legitimate purpose," *id.* at 202 (Rule 37), is significant, as described throughout Part III.

19. *See, e.g.*, Bill, *supra* note 15, at 59 (noting that the international community is consistently expanding human rights law).

20. TALLINN MANUAL 2.0, *supra* note 2, at 187 (Rule 35).

21. *Id.* at 189.

22. *Id.*

23. International human rights laws are designed "to induce states to remedy the inadequacies of their national laws and institutions," thus ensuring these individual protections are "respected and vindicated." Louis Henkin, *Introduction* to THE INTERNATIONAL BILL OF RIGHTS: THE COVENANT ON CIVIL AND POLITICAL RIGHTS 14 (Louis Henkin ed., 1981).

24. *See* TALLINN MANUAL 2.0, *supra* note 2, at 196 (Rule 36) (requiring State actors to respect and protect international human rights).

25. "Derogation refers to the legal right to suspend certain human rights treaty provisions in time of war or in cases of national emergencies. Certain fundamental (customary law) rights, however, may not be derogated from . . . ." DESKBOOK, *supra* note 16, at 205 (emphasis omitted).

and the right to recognition as a person before the law,[26] the International Group of Experts notes that privacy "is not an absolute right and may be subject to limitations, as discussed in Rule 37."[27] Thus, Rule 37—"[t]he obligations to respect and protect international human rights, with the exception of absolute rights, remain subject to certain limitations that are necessary to achieve a legitimate purpose, nondiscriminatory, and authorized by law"—offers a methodology for limiting the international human right of privacy in cyberspace.[28]

As a final background matter for purposes of this Article, the International Group of Experts outlines the effect of secrecy as a barrier to understanding State practice in cyberspace, arguing that "State cyber practice is mostly classified and publicly available expressions of *opinio juris* are sparse, [making it] difficult to definitively identify any cyber-specific customary international law."[29] While this statement accurately captures aspects of the contemporary environment, specific State practice in cyberspace is increasingly available to the public[30] and, in time, can ripen into customary international law. Though not yet at the level of customary

---

26. *See* G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948) (listing human rights to which all people are entitled and denying recognition of any State right to "engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms set forth herein"). For a discussion on whether the Universal Declaration has ripened into customary international law, see Hurst Hannum, *The Status of the Universal Declaration of Human Rights in National and International Law*, 25 GA. J. INT'L & COMP. L. 287, 317–52 (1996). The same prohibition on derogation applies in the cyber context. TALLINN MANUAL 2.0, *supra* note 2, at 208. However, the *Manual* differentiates between the impermissibility of limiting a human right and the notion of nonderogability. *Id.* at 202–03.

27. TALLINN MANUAL 2.0, *supra* note 2, at 189.

28. *Id.* at 201–02. Cyberspace is defined as "a global domain within the information environment that encompasses the interdependent networks of information technology infrastructures, including the Internet and telecommunication networks." U.S. DEP'T OF DEF., QUADRENNIAL DEFENSE REVIEW REPORT 37 (2010) [hereinafter DEFENSE REVIEW REPORT]. *Tallinn Manual 1.0* defines cyberspace as "[t]he environment formed by physical and non-physical components, characterized by the use of computers and the electro-magnetic spectrum, to store, modify, and exchange data using computer networks." TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 258 (Michael Schmitt ed., 2013) [hereinafter TALLINN MANUAL 1.0].

29. TALLINN MANUAL 2.0, *supra* note 2, at 3.

30. Some States share this information by choice. *See, e.g.*, JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-12(R): CYBERSPACE OPERATIONS (2013) [hereinafter JOINT PUBLICATION 3-12(R)], http://www.dtic/mil/doctrine/new_pubs/jp3_12R.pdf [https://perma.cc/RH4E-DHTA] (describing the United States' military operations in and through cyberspace in an unclassified document easily accessible over the Internet). In other instances, States' cyber activities are being exposed. *See, e.g.*, Daniel Garrie & Shane R. Reeves, *An Unsatisfactory State of the Law: The Limited Options for a Corporation Dealing with Cyber Hostilities by State Actors*, 37 CARDOZO L. REV. 1827, 1829–30, 1835–36 (2016) (discussing a number of unattributed cyber acts conducted by State actors); Frank Langfitt, *U.S. Security Company Tracks Hacking to Chinese Army Unit*, NPR (Feb. 19, 2013), http://www.npr.org/2013/02/19/172373133/report-links-cyber-attacks-on-u-s-to-chinas-military [https://perma.cc/L87Z-RJ9M].

international law, certain State practice in cyberspace, and a discussion of its relevance, are key subjects to which this Article returns below.

II. Is Countering Terrorism a Legitimate Reason to Violate the Right to Privacy in Cyberspace?

Importantly, Rule 37 of the IHRL Chapter states that the "obligations to respect and protect international human rights, with the exception of absolute rights, remain subject to certain limitations."[31] Recognizing the sensitivity of placing limitations on international human rights, Rule 37's commentary expounds on the limitation criteria and their applicability.[32] While the International Group of Experts discusses the need to ground any limitation in international law[33] and for these measures to be nondiscriminatory,[34] the greatest ambiguity in the applicability of Rule 37 surrounds the meaning of "legitimate purpose." In an effort to establish parameters for whether a limitation serves a legitimate purpose, the International Group of Experts offers in the commentary a nonexhaustive list of legitimate purposes, including: "protection of rights and reputations of others, national security, public order, public health, [and] morals."[35] To provide even a greater understanding of the term, the commentary gives an example: "For instance, countering terrorism is a legitimate purpose that allows States to monitor particular online communications without thereby violating the right to privacy."[36]

Despite the admirable attempt of the International Group of Experts to define a "legitimate purpose," the term remains overly broad. The commentary's countering-terrorism example most starkly illustrates this point. Currently, there is no universally accepted definition of "terrorism,"[37]

---

31. TALLINN MANUAL 2.0, *supra* note 2, at 201–02.

32. *Id.* at 202–03.

33. *See id.* at 202 ("[T]he basis for a limitation on the enjoyment or exercise of an international human right must be provided for in international law.").

34. *See id.* at 206 ("Restrictions on cyber activities that are otherwise protected by international human rights law must be non-discriminatory.").

35. *Id.* at 203.

36. *Id.*

37. Since 1996, an effort within the United Nations has been ongoing to develop the Comprehensive Convention on International Terrorism. G.A. Res. 51/210, ¶ 9 (Dec. 17, 1996) (establishing an ad hoc committee to develop "a comprehensive legal framework of conventions dealing with international terrorism"). However, the negotiations are consistently deadlocked due to disagreements over the definition of the term. *See Ad Hoc Committee Established by General Assembly Resolution 51/210 of 17 December 1996*, UNITED NATIONS OFF. LEGAL AFFAIRS, http://legal.un.org/committees/terrorism/ [https://perma.cc/S5JU-CCMD] (outlining the ongoing emphasis on developing the treaty in order to eliminate international terrorism); Press Release, General Assembly, Legal Committee Urges Conclusion of Draft Comprehensive Convention on International Terrorism, U.N. Press Release GA/L/3433 (Oct. 8, 2012) (urging an agreement on a clear definition of "terrorism").

and the parameters of the term remain contentiously debated.[38] As a result, there is a myriad of national and regional definitions for "terrorism."[39] The closest the international community has come to an understanding of the concept is in United Nations Security Council Resolution 1566, which forbids:

> criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act . . . .[40]

The resolution, however, is unhelpful as it is nonbinding and lacks authority in international law.[41] Further, its offered definition of "terrorism" is sufficiently vague to allow for individual State interpretations. "Terrorism," therefore, can encompass a wide range of activities and, in its nebulous conception, is highly susceptible to States' infringement on individuals' right of privacy in cyberspace.

Similarly, the broad concept of "countering terrorism" is too expansive to be a "legitimate purpose." "Counterterrorism," like "counterinsurgency,"[42] is a far-reaching strategic term that is expansively applied to a variety of circumstances. Described by the United States as "activities and operations . . . taken to neutralize terrorists, their organizations, and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their

---

38. *See* ANGUS MARTYN, AUSTL. DEP'T PARLIAMENTARY LIBRARY, THE RIGHT OF SELF-DEFENCE UNDER INTERNATIONAL LAW—THE RESPONSE TO THE TERRORIST ATTACKS OF 11 SEPTEMBER 3 (2002), http://www.aph.gov/au/binaries/library/pubs/civ/2001-02/02cib08.pdf [https://perma.cc/DSR3-7ADK] ("The international community has never succeeded in developing an accepted comprehensive definition of terrorism."); James Hess, *The Challenge of Defining Terrorism Around the World*, IN PUBLIC SAFETY (July 13, 2015), http://inpublicsafety.com/2015/07/the-challenge-of-defining-terrorism-around-the-world/ [https://perma.cc/XG8R-U3AV] ("Those familiar with the study of terrorism know there is not a universally accepted definition.").

39. Alex P. Schmid, *The Revised Academic Consensus Definition of Terrorism*, 6 PERSP. ON TERRORISM 158, 158 (2012), http://www.terrorismanalysts.com/pt/index/php/pot/article/view/schmid-terrorism-definition/385 [https://perma.cc/HTV7-LURW].

40. S.C. Res. 1566, ¶ 3 (Oct. 8, 2004).

41. Schmid, *supra* note 39, at 158.

42. Counterinsurgency (COIN) is described by the United States as "a comprehensive civilian and military effort designed to simultaneously defeat and contain insurgency and address its root causes. COIN is primarily a political struggle and incorporates a wide range of activities by the [host-nation] government of which security is only one, albeit an important one." JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-24: COUNTERINSURGENCY I-2 (2013) [hereinafter JOINT PUBLICATION 3-24], www.dtic.mil/doctrine/new_pubs/jp3_24.pdf [https://perma.cc/MDY5-3D7P].

goals," the concept is intentionally broad to allow for a variety of responses.[43] Countering terrorism, in other words, is whatever a State does to "disrupt, isolate, and dismantle terrorist organizations."[44] Admittedly, States are obligated to comply with international human rights law when implementing their counterterrorism measures.[45] However, this obligation lacks specificity and allows wide latitude to States in determining how to "counter terrorism," including, if necessary, monitoring online personal communications.

Declaring that "countering terrorism" is a "legitimate purpose" for infringing upon the right to privacy in cyberspace is both vague and problematic. Equally troubling is the use of other broad and amorphous terms such as "national security," "public order," or "public health" to describe a "legitimate purpose."[46] By leaving the description of a "legitimate purpose" vague, Rule 37 gives State actors discretion, increasing the risk of overzealous limitations on international human rights in the cyber context. To its credit, the International Group of Experts does not ignore this problem and addresses this concern by emphasizing in the commentary that "[a] restriction on cyber activities that might otherwise be protected by international human rights law must be 'necessary.'"[47] However, this language is of questionable impact as the commentary immediately follows with the statement "although States enjoy a margin of appreciation in this regard."[48]

The International Group of Experts also raises the principle of proportionality, as it applies to limiting international human rights, as a check on overuse of Rule 37.[49] The idea of proportionality is extensively used throughout international law;[50] thus, it is helpful for the commentary to note

---

43. *See* JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-26: COUNTERTERRORISM I-5 (2014) [hereinafter JOINT PUBLICATION 3-26], www.dtic.mil/doctrine/new_pubs/jp3_26.pdf [https://perma.cc/C5XD-Q5CL] (providing guidance to U.S. armed services for counterterrorism activities).

44. *Id.* at I-6.

45. *See* S.C. Res. 1624, ¶ 4 (Sept. 14, 2005) (requiring that States "comply with all of their obligations under international law, in particular international human rights law, refugee law, and humanitarian law" when conducting counterterrorism operations); *Terrorism/Counterterrorism*, HUMAN RIGHTS WATCH, https://www.hrw.org/topic/terrorism-counterterrorism [https://perma.cc/4SST-N6UB] ("Governments have a responsibility to protect those within their jurisdiction from extremist attacks, but must ensure that all counterterrorism measures respect human rights.").

46. TALLINN MANUAL 2.0, *supra* note 2, at 203.

47. *Id.*

48. *Id.*

49. *Id.* at 204–05.

50. For example, proportionality is one of the principles of the law of armed conflict. *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (Protocol I) art. 51(5)(b), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I] (noting that proportionality determines whether "an attack . . . may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a

expressly "that the need for any State interference with human rights in order to meet a legitimate State objective be assessed against the severity of the infringement on human rights."[51] The commentary goes on to state that the restriction must be the least intrusive means available to achieve the stated objective.[52] While disagreeing as to whether the proportionality principle is customary, the Experts note in the commentary that a majority "accepted a condition of proportionality."[53] In so doing, they agreed that "necessity alone does not suffice to justify limiting obligations" as it would be "incongruent with the object and purpose of limitations on international human rights law to permit a restriction that is necessary, but disproportionate to the State's interest in question."[54] Yet, again, after outlining this seeming restraint, the commentary goes on to note that State actors "enjoy a margin of appreciation" when applying the least-restrictive-means proportionality requirement.[55]

Rule 37 and its commentary consistently defer to States. This deference allows the State to determine unilaterally whether a limitation on an international human right in cyberspace is necessary to achieve a legitimate purpose and, if so, how to effectuate any limitations in a proportional manner. The vague and broad terminology used to describe a "legitimate purpose" further empowers the State to limit human rights in the cyber context if it so chooses. The Experts' use of generalities, including but not limited to the term "countering terrorism," and the deference shown to States throughout Rule 37, therefore leaves open the question of what exactly restrains a State from limiting international human rights in cyberspace.

III. Do Not Worry . . . State Practice Will Begin to Fill the Gaps

The uncertainty in Rule 37 is not surprising, as a granular analysis of such an ambitious and unprecedented project as the *Manual* will invariably reveal some gaps. This is similar to *Tallinn 1.0*,[56] which, in its attempt "to

combination thereof [that would] be excessive in relation to the concrete and direct military advantage anticipated").

51. TALLINN MANUAL 2.0, *supra* note 2, at 204.

52. *Id.*

53. *Id.* at 205.

54. *Id.*

55. *Id.*

56. The *Tallinn Manual on the International Law Applicable to Cyber Warfare* was drafted to help governments "deal with the international legal implications of cyber operations." 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, 648 (2013); *see also* Jeremy Kirk, *Manual Examines How International Law Applies to Cyberspace*, IT WORLD (Sept. 3, 2012), http://www.itworld.com/article/2720628/it-management/manual-examines-how-international-law-applies-to-cyberwarfare.html [https://perma.cc/P8E6-JB7L] (reporting that the original *Tallinn Manual* was created by The Cooperative Cyber Defense Center of Excellence, which "assists NATO

explain how the existing law of armed conflict generally regulate[d] cyber warfare," left certain specifics unaddressed.[57] For example, *Tallinn 1.0*'s Rule 27 states that "[i]n an international armed conflict, inhabitants of unoccupied territory who engage in cyber operations as part of a *levée en masse* enjoy combatant immunity and prisoner of war status."[58] Yet this attempt "to reconcile the [traditional] concept of *levée en masse*[59] with the 'cyber conflicts between nations and ad hoc assemblages'" is simply impractical.[60] While there are a number of problems with the idea of a cyber *levée en masse*,[61] the most obvious is the traditional criteria that those participating in a spontaneous uprising carry arms openly.[62] The requirement to "carry[] arms openly" is of utmost importance in a *levée en masse* as these movements are done in emergency circumstances, leaving no time for organization or for participants to use distinctive signs.[63] With no other form of recognition, carrying a weapon becomes the "only distinguishing characteristic between a protected civilian and a combatant, and, therefore, who can be lawfully attacked."[64] Further, there is no question as to what "carrying arms openly" means for those participating in a *levée en masse*.

---

with technical and legal issues associated with cyberwarfare-related issues" in order to address a variety of cyber legal issues).

57. *See* Wallace & Reeves, *supra* note 56, at 648–49 (arguing that *Tallinn 1.0*'s application of the existing law of armed conflict to cyber warfare was too general to adequately address the problems of cyber warfare).

58. TALLINN MANUAL 1.0, *supra* note 28, at 102.

59. A *levée en masse* occurs when inhabitants of a nonoccupied territory, without time to form into a regular armed unit, spontaneously take up arms to resist an invading force. Those that take up arms forfeit their civilian status and become combatants. *See* Geneva Convention Relative to the Treatment of Prisoners of War art. 4(A)(6), Aug. 12, 1949, 6 U.S.T. 3316; GARY D. SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR 200–01 (2010) (quoting the definition of *levée en masse* as stated in Prosecutor v. Delalić, Case No. IT-96-21-T, Judgment, ¶ 268 (Int'l Crim. Trib. for the Former Yugoslavia Nov. 16, 1998)). The idea behind a *levée en masse* is simple: during an invasion, the civilian population of unoccupied territory can spontaneously take up arms against the invading army to stop an occupation. YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 42 (1st ed. 2004).

60. *See* Wallace & Reeves, *supra* note 56, at 649 (quoting Stephen W. Korns & Joshua E. Kastenberg, *Georgia's Cyber Left Hook*, PARAMETERS, Winter 2008–09, at 60, 70).

61. *See id.* at 658–60 (discussing how the traditional occupied–unoccupied paradigm and mass-uprising aspects of a *levée en masse* are less relevant in the cyber context).

62. A *levée en masse* is expected to be a spontaneous uprising where inhabitants impulsively organize and are only distinguished as combatants by the open and visible carrying of arms. *See* COMMENTARY, III GENEVA CONVENTION RELATIVE TO THE TREATMENT OF PRISONERS OF WAR 67 (Jean S. Pictet ed., 1960) [hereinafter COMMENTARY, GC III] (explaining that the requirement of open carry is intended to protect the "combatants themselves who must be recognizable in order to qualify for treatment as prisoners of war").

63. Wallace & Reeves, *supra* note 56, at 657.

64. *Id.*

The referred-to arms are clearly traditional weapons like rifles, hand grenades, and pistols.[65]

"Recognizing both the realities of a *levée en masse* and the criticality of protecting civilians, the law of armed conflict [thus] places singular emphasis on the essential need for those choosing to participate in a spontaneous uprising" to openly carry these conventional armaments.[66] Yet, in a cyber *levée en masse* the "weapon" used is a computer. While it is possible for a computer to be considered a "weapon,"[67] simple possession "cannot be interpreted to be indicative of combatant activity."[68] The *Tallinn 1.0* International Group of Experts recognized this reality by noting, "even if [computers] qualify as weapons, the requirement to carry arms openly has little application in the cyber context."[69] A detailed law of armed conflict (LOAC) analysis reveals key challenges related to this area: namely, the impossibility of distinguishing participants in a cyber *levée en masse* and, subsequently, the inability of participating individuals to comply with the required LOAC principle of distinction.[70]

The *Tallinn 1.0* International Group of Experts understood the difficulties with the concept of a cyber *levée en masse* and even "highlight[ed] various unanswered and troubling questions in the commentary to Rule 27."[71] The Experts were also aware that a general application of the existing LOAC to cyber warfare does not always work[72] and future legal developments are necessary to address the nuanced issues

---

65. *See* COMMENTARY, GC III, *supra* note 62, at 61 (discussing the requirement of carrying arms openly, referring to weapons such as hand grenades or revolvers).

66. Wallace & Reeves, *supra* note 56, at 657.

67. *Tallinn 1.0* defines a cyber weapon as "cyber means of warfare that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of, objects, that is, causing the consequences required for qualification of a cyber operation as an attack." TALLINN MANUAL 1.0, *supra* note 28, at 141–42.

68. Wallace & Reeves, *supra* note 56, at 659.

69. TALLINN MANUAL 1.0, *supra* note 28, at 100.

70. The principle of distinction states that "[i]n order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives." AP I, *supra* note 50, art. 48. For additional discussions on applying the principle of distinction in cyberspace, see Robin Geib & Henning Lahmann, *Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space*, 45 ISR. L. REV. 381, 384 (2012) (theorizing that nonmilitary components of cyberspace itself will become targets of cyberwarfare operations); Noam Lubell, *Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?*, 89 INT'L L. STUD. 252, 264 (2013) (recognizing complicated questions surrounding the threshold level of harm required for cyber operations to become "attacks" subject to the LOAC).

71. Wallace & Reeves, *supra* note 56, at 658–59; *see also* TALLINN MANUAL 1.0, *supra* note 28, at 102–03 (discussing various problems with the concept of a cyber *levée en masse* and the limited circumstances in which it would apply).

72. *See* Wallace & Reeves, *supra* note 56, at 649 (noting that a cyber *levée en masse* "illustrates how ill-suited, and often impractical, the existing law of armed conflict can be when applied in the cyber context").

generated by the novelties of cyber warfare.[73] Yet, due to "the relative infancy of cyber operations and paucity of state practice,"[74] the *Tallinn 1.0* International Group of Experts only addressed the "law currently governing cyber conflict."[75] Avoiding theoretical debates,[76] *Tallinn 1.0* thus provided a general regulatory framework capable of allowing the LOAC to evolve, as necessary, to address the unanticipated complexities that emerge in cyberspace.[77]

Similar to *Tallinn 1.0*, *Tallinn 2.0*'s IHRL Chapter acts as a broad foundational document that intentionally leaves room for further legal developments. As noted in Part III, the International Group of Experts occasionally refers to terms without adding specificity to their meaning. For example, the commentary to Rule 36 states:

> The Internet has been used for terrorist purposes, such as recruitment for, incitement of, and the financing of terrorism. The International Group of Experts agreed that "States have both a right and a duty to take effective measures to counter the destructive impact of terrorism on human rights," even though some measures taken by the State may affect human rights such as the freedom of expression and the right of privacy. Any such measures must comply with Rule 37.[78]

Like the term "legitimate purpose" in the commentary to Rule 37, the Rule 36 language leaves open a critical question—namely, what constitutes "effective measures" States have a right and duty to undertake in this context? Moreover, what is an effective measure that rises to the level of a legitimate purpose for limiting the international human right of privacy in the cyber context?[79]

The United States has begun to answer this question by publicly advertising the measures it employs to "counter terrorism" in cyberspace. The United States requires "[i]nformation-related capabilities such as . . . cyberspace operations . . . [to] be applied to [counterterrorism] operations as

---

73. TALLINN MANUAL 1.0, *supra* note 28, at 5 (noting that the *Manual* does not cover best practices or preferred policies); *see also* Schmitt, *supra* note 5, at 274 (noting that for States to be successful in cyberspace they will need to depart from "the received norms that have been set forth by the International Group of Experts in the *Tallinn Manual*").

74. Schmitt, *supra* note 5, at 270.

75. TALLINN MANUAL 1.0, *supra* note 28, at 5.

76. The 95 "Black Letter Rules" of *Tallinn 1.0* still "sometimes evoked ardent and nuanced debate," with the "commentary accompanying each Rule captur[ing] these debates and highlight[ing] those which remain unresolved." Schmitt, *supra* note 5, at 271.

77. *See, e.g.*, DEFENSE REVIEW REPORT, *supra* note 28, at 62 (noting that rising complexities in cyberspace "pose new security challenges that require innovative adjustments to our defense posture").

78. TALLINN MANUAL 2.0, *supra* note 2, at 199.

79. *See supra* notes 34–36 and accompanying text (discussing the nature of a "legitimate purpose" as a justification for restricting international rights).

a means to influence extremists, their supporters, and the mainstream populace."[80] These cyber operations, nested within the United States' counterterrorism efforts, are "composed of the military, intelligence, and ordinary business operations of [the Department of Defense] in and through cyberspace."[81]

While this broad definition of cyberspace operations may not be tremendously helpful, Joint Publication 3-12(R), an unclassified military document titled "Cyberspace Operations," provides some clarity. The document notes that "successful execution of [cyberspace operations] requires the integrated and synchronized employment of offensive, defensive, and DODIN operations, underpinned by effective and timely operational preparation of the environment [(OPE)]."[82] It goes on to state that categorization of a cyberspace operation is dependent upon the intent behind the mission.[83] However, "these missions . . . require the employment of various capabilities to create specific effects," and therefore the document discusses a number of particular actions in cyberspace.[84]

In so doing, it becomes possible to determine what type of cyber activities are considered part of "cyberspace operations" and subsequently are included as cyberspace measures in United States counterterrorism operations. Cyberspace Intelligence, Surveillance, and Reconnaissance (C-ISR), which gathers intelligence to support a future offensive or defensive cyber operation[85] and maps adversary cyberspace to support military planning,[86] is one example of a listed activity. Additionally, cyberspace operational preparation of the environment (C-OPE), which "consists of the non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations,"[87] is also a described cyber action.

---

80. JOINT PUBLICATION 3-26, *supra* note 43, at V-6.

81. JOINT PUBLICATION 3-12(R), *supra* note 30, at vii.

82. *Id.* Offensive cyber operations (OCO) are "intended to project power by the application of force in and through cyberspace." *Id.* Defensive cyber operations (DCO) are "intended to defend DOD or other friendly cyberspace." *Id.* The Department of Defense Information Network (DoDIN) "is a global infrastructure of Department of Defense (DOD) systems carrying DOD, national security, and related intelligence community information and intelligence." *Id.* at vi.

83. *Id.* at vii.

84. *Id.* at II-4 to -5.

85. *Id.*

86. *Id.* C-ISR "requires appropriate deconfliction, and cyberspace forces that are trained and certified to a common standard with the [intelligence community]. ISR in cyberspace is conducted pursuant to military authorities and must be coordinated and deconflicted with other [United States Government] departments and agencies." *Id.*

87. *Id.* at II-5. Operational preparation of the environment is defined as "[t]he conduct of activities in likely or potential areas of operations to prepare and shape the operational environment." JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-05: SPECIAL OPERATIONS GL-9 (2014), www.dtic.mil/doctrine/new_pubs/jp3_05.pdf [https://perma.cc/3SMP-SFYN].

Some of the described actions, such as "cyberspace attack,"[88] clearly cross the use-of-force threshold and would not be regulated by the international law contemplated in *Tallinn 2.0*.[89] However, C-ISR and C-OPE most likely fall below the use-of-force line as, by definition, they do not cause damage, injury, or even severe nonphysical consequences.[90] Instead, these cyber activities focus on intelligence gathering and planning for future military operations, both of which are peacetime activities. As a result, it becomes possible to start determining what cyber measures below the use of force the United States employs to counter terrorism.

Understanding what cyber activities below the use-of-force threshold the United States employs in its counterterrorism efforts thus helps to define the term "effective measure" as undertaken in the Rule 36 context. More importantly, it evinces State practice and begins to represent the legal developments necessary to fill in the gaps left open by *Tallinn 2.0*'s IHRL Chapter. Of course, the United States' practice is a singular example of one nation's behavior and is clearly not a customary norm. Yet it is an important representation of how State practice can provide the specificity currently missing in *Tallinn 2.0* while simultaneously illustrating how the international law regulating cyber operations is likely to develop in the future.

---

88. Cyberspace attack is defined as "[c]yberspace actions that create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains." JOINT PUBLICATION 3-12(R), *supra* note 30, at II-5. *Deny*, *degrade*, and *disrupt* are all defined. *See id.*

89. Of course, these activities must fall below the use-of-force threshold for *Tallinn 2.0* to apply. "[S]tates and scholars have struggled mightily to define the threshold at which an act becomes a 'use of force.'" Schmitt, *supra* note 5, at 279. While there is no bright-line test that determines if a cyber operation is a use of force, there are a number of factors that inform this determination. *See id.* at 280 (enumerating these factors). The *Tallinn 1.0* International Group of Experts created a nonexhaustive list that includes:

> severity, immediacy, directness, invasiveness, measurability, military character, state involvement, and presumptive legality. Additional factors found meaningful by the Experts included, inter alia, the prevailing political environment, the nexus of an operation to prospective military force, the attacker's identity, the attacker's track record with respect to cyber operations, and the nature of the target. These and other factors operate in concert as [S]tates make case-by-case determinations. Of them, only severity alone can qualify a cyber operation as a use of force.

Id. at 280–81 (citing TALLINN MANUAL 1.0, *supra* note 28, at 47–52).

90. However, these activities may potentially violate the territorial sovereignty of a State. For additional discussion on this topic, see Garrie & Reeves, *supra* note 30, at 1857–58 (discussing how cyber actions that fall below the use-of-force threshold may still violate international law). Regardless, such actions would still be regulated by *Tallinn 2.0*. *See* TALLINN MANUAL 2.0, *supra* note 2, at 1 (noting *Tallinn 2.0*'s inclusion of "the public international law governing cyber operations during peacetime" in order to address "cyber issues that lie below the use of force threshold").

IV. Conclusion

Similar to *Tallinn 1.0*, *Tallinn 2.0* is an unprecedented attempt to codify international law, albeit below the use-of-force threshold, in cyber operations.[91] It is an objective restatement of the *lex lata*, versus a reflection of *lex ferenda*,[92] for the same reason *Tallinn 1.0* only analyzed current international law: namely, to avoid making questionable predictions about how the law should develop.[93] Instead, the International Group of Experts behind *Tallinn 2.0*, and specifically its International Human Rights Law Chapter, created a foundational document with room for international law to develop and fill gaps as needed.[94] This "gap filler" will come in the form of either a treaty or by States' "engaging in practices out of a sense of legal obligation (*opinio juris*) that, combined with similar practice by other [S]tates, eventually crystallizes into customary international law."[95] With the accelerating pace of change in cyberspace[96] and the glacial speed at which conventional law develops,[97] new international law will likely come through State practice.

Although certain terms in the IHRL Chapter generally—and in Rules 36 and 37, specifically—are problematic, both the IHRL Chapter and the *Tallinn Manual 2.0* represent a tremendously useful starting point for assessing the challenging intersection of multiple areas of the law. Quickly filling definitional gaps is essential to amplifying the Chapter and determining what legitimate reasons may exist to violate rights, such as privacy, in cyberspace. Moreover, understanding timely, relevant activities not triggering the law of armed conflict but nevertheless of the type contemplated throughout *Tallinn*

---

91. *See* TALLINN MANUAL 2.0, *supra* note 2, at 1 (noting that *Tallinn 2.0* is a "follow-on initiative to expand the Manual's scope to include the public international law governing cyber operations during peacetime").

92. *Id.* at 2–3. *Lex lata* is defined as "what the law is." J. Jeremy Marsh, Lex Lata *or* Lex Ferenda*? Rule 45 of the ICRC Study on Customary International Humanitarian Law*, 198 MIL. L. REV. 116, 117 (2008). *Lex ferenda* is defined as "what the law should be." *Id.*

93. *See* TALLINN MANUAL 2.0, *supra* note 2, at 3 ("[T]he Experts involved in both projects [*Tallinn 1.0* and *2.0*] assiduously avoided including statements reflecting *lex ferenda*."); Schmitt, *supra* note 5, at 271 ("Adding to the uncertainty regarding the precise legal parameters of cyber warfare is the fact that public international law is by nature a dynamic creature. . . . [I]ts content, interpretation, and application evolve over time in response to transformation of the security environment in which it applies.").

94. *See* Schmitt, *supra* note 5, at 299 ("International law is designed to govern the present and shape the future.").

95. *Id.* at 272–73 (citing Statute of the International Court of Justice art. 38(1), June 26, 1945, 59 Stat. 1055).

96. *See* DEFENSE REVIEW REPORT, *supra* note 28, at iii (discussing how the "pace of change continues to accelerate" in modern warfare).

97. *See* TALLINN MANUAL 2.0, *supra* note 2, at 3 ("There are very few treaties that directly deal with cyber operations and those that have been adopted are of limited scope.").

2.0, such as the United States' C-ISR and C-OPE efforts, serve as tremendous indicators of State practice in this area.

Finally, it must be stated that the above nuanced criticism is not a broad condemnation of the Group of Experts' efforts in any regard. To the contrary, it is only because of their excellent and unprecedented work that we are able to spot the definitional gaps and begin to fill them with evidence of State practice. All of it, and especially the IHRL Chapter, represents a tremendous contribution to the law.