2016

# Interpretation Catalysts in Cyberspace

Rebecca Ingber

# Interpretation Catalysts in Cyberspace

Rebecca Ingber*

## Introduction

The cybersphere offers a rich space from which to explore the development of international law in a compressed time frame. Rapidly advancing capabilities and novel events distill and sharpen longstanding debates in international law: questions involving how the law adapts to new technologies; disagreement over the extent to which secret action can move custom;[1] disputes over the need for heightened transparency;[2] and power wrangling between states and soft law endeavors in driving the development of the law. In particular, the continuously evolving need to determine how existing laws apply to shifting capabilities provides fertile ground for innovative legal positioning and interpretation. That constant innovation in turn creates opportunities for discrete triggers for legal interpretation—or "interpretation catalysts" as I have termed them elsewhere[3]—to influence the path that legal evolution takes. Interpretation catalysts not only compel a decision-making body to take a position on its interpretation of a legal rule; they shape all aspects of the decision-making process, ultimately influencing the legal position that body takes, and often the resulting law itself.[4]

In this generative space of cyber law, the *Tallinn Manual* processes of the past ten years provide a valuable lens through which to witness the effects of interpretation catalysts on the evolution of international law. The *Tallinn* processes have been remarkable achievements, both in producing manuals that navigate the web of international laws regulating state action in cyberspace, and in driving states to consider and to continue to develop the

---

* Associate Professor, Boston University School of Law. Many thanks to Susan Akram, Pamela Bookman, Daniela Caruso, Ashley Deeks, Kristen Eichensehr, Dustin Lewis, Dinah PoKempner, Naz Modirzadeh, Robert Sloane, and Phil Spector for invaluable conversations and comments on drafts. I am grateful to Stew Sibert for excellent research assistance.

1. Alexandra H. Perina, *Black Holes and Open Secrets: The Impact of Covert Action on International Law*, 53 COLUM. J. TRANSNAT'L L. 507, 511 (2015).

2. Harold H. Koh, *The Legal Adviser's Duty to Explain*, 41 YALE J. INT'L L. 189, 189–90 - (2016).

3. *See* Rebecca Ingber, *Interpretation Catalysts and Executive Branch Legal Decisionmaking*, 38 YALE J. INT'L L. 359, 360 (2013) (identifying the concept of "interpretation catalysts," and demonstrating their role in triggering distinct processes within the executive branch for formulating legal positions).

4. *Id.* at 377.

rules governing this space. The two *Tallinn Manuals*[5] lay out for states not only an experts' sense of where consensus on the law currently stands, but also—and just as importantly—the parameters of precisely where the disagreements among states may lie, where there might be room for movement, and what the outer parameters of that movement might be. And for academics, the *Tallinn* processes also provide a unique case study to consider the development of international law over a short period of time and the influence of soft law processes on that development.

In particular, the *Tallinn Manual* processes and resulting manuals provide insight into how these "interpretation catalysts," or discrete triggers for legal interpretation, influence the path that legal evolution takes.[6] The operative interpretation catalyst triggering the need for a legal decision influences every aspect of decision making from the identity of the particular players involved in an interpretative endeavor to the task before them, the context in which they operate, and the investment in the project by the relevant players.[7] In the *Tallinn* processes, those players have included not only the experts around the drafting table but also states watching and engaging from the sidelines. All of these factors shape where the law—or the interpretation of the law—ultimately lands.[8]

In prior work, I have explored the phenomenon of "interpretation catalysts" through the lens of state decision making, specifically U.S. executive branch legal decision making on matters of national security.[9] In that context, the lack of external checks on the U.S. President often means that the executive branch legal position is virtually the only operative legal constraint.[10] The interpretation catalyst driving such executive branch decision making therefore has an enormous influence not just on one party's opening legal position but on the governing law itself.[11]

In the case of the *Tallinn* processes, as I will elaborate in Part II, interpretation catalysts operate on two levels. The initial interpretation catalyst, the Estonia cyberattacks, impelled states to consider the applicable legal framework to apply to those attacks. Most significantly for our

---

5. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael Schmitt ed., 2013) [hereinafter TALLINN MANUAL]; TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0].

6. Ingber, *supra* note 3, at 377 (identifying and exploring the role of "interpretation catalysts" in driving decision making in the context of U.S. executive branch legal interpretation).

7. *See id*.

8. *See id*.

9. *See id*.

10. *See id*.

11. *Id.*

purposes, those events triggered the initiation and development of the first *Tallinn Manual* process itself, thus setting those wheels in motion.[12] Second, both *Tallinn* processes have themselves acted and continued to act as interpretation catalysts for states, compelling them—often intentionally—to develop their positions on the legal rules governing cyberspace. As I will touch on below as well, this case study illustrates not only how distinct events can trigger and shape the path of legal interpretation, but also that these triggers are not fixed; the power inherent in interpretation catalysts suggests that they may also be manipulated to push the law toward desired ends.

Now, I should acknowledge up front that the stated intent of the *Manual*'s drafters is not to drive the law but rather to lay out the current areas of legal consensus and of continued debate.[13] And yet the drafters also evince a clear intent to push states "proactively" toward development of the law themselves as well as in conjunction with the project.[14] A state legal adviser could not fail to notice that if states do not start working together to hammer out the rules governing this space, there is a risk these non-state-driven projects will continue to outpace them and ultimately may nudge the law in directions that states do not necessarily wish it to go.[15] It is for that very reason that the Dutch government sponsored "The Hague Process," a major convening of states, in order to review and comment on the *Tallinn Manual 2.0* while that process was underway.[16]

As states participating in The Hague Process no doubt concluded, it would be naïve to assume that the *Tallinn* processes would have no effect on development of the law. It is worth, then, pausing to consider the direction

12. *See infra* notes 45–48 and accompanying text.

13. Michael Schmitt, Tallinn Manual 2.0 on the International Law of Cyber Operations*: What It Is and Isn't*, JUST SECURITY (Feb. 9, 2017), https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations [https://perma.cc/Z7ZA-QXKN].

14. *See id.* (explaining the virtues of clarity in the law regulating state action, in, *inter alia*, "lend[ing] stability to international relations" and "help[ing] deter other states from exploiting . . . grey zones in the law of cyberspace"); Tallinn Manual *Experts Meet for Intense Drafting Session*, NATO COOP. CYBER DEF. CTR. EXCELLENCE, 2:55–3:20 (Oct. 9, 2015), https://ccdcoe.org/tallinn-manual-20-be-completed-2016.html [https://perma.cc/EY2S-MKTD] (interviewing Tim McCormack, Professor of Law at the University of Melbourne, who explains that states are often "reactive to new . . . developments" and that *Tallinn 2.0* is an effort "to gather a group of experts together to proactively clarify the state of the law in an area that states are still asking questions about what law is going to apply").

15. *See* Schmitt, *supra* note 13 (noting that participants in the *Tallinn* process intended "that it would enhance the process of norm identification and elucidation by states"); Michael J. Adams, *A Warning About* Tallinn 2.0 . . . *Whatever It Says*, LAWFARE (Jan. 4, 2017), https://www.lawfareblog.com/warning-about-tallinn-20-. . .-whatever-it-says [https://perma.cc/92R7-RAM9] (expressing concern that users of the *Tallinn* manuals may inappropriately conclude that the law in certain areas is more settled than states have in fact themselves determined).

16. *See* Schmitt, *supra* note 13 (describing "The Hague Process").

that such a project might push the law and indeed quite likely already has. I do not take a strong normative position in this piece on the specific direction cyber law has taken during the course of this project, other than to recognize the benefits of clarity in the law for state actors and others interested in the rule of law and in public law more generally. My intended contribution here is primarily to highlight the strong influence of the triggers for legal interpretation on decision-making processes, on the legal positions coming out of those processes, and thus, on the ultimate development of the law. The *Tallinn* processes—and specifically the second *Tallinn* process's treatment of international human rights law as contrasted with its treatment of the law of armed conflict—form an invaluable case study to examine the role of interpretation catalysts in legal interpretation.

## I. Human Rights in Cyber Law

Both of the *Tallinn* processes and their ultimate products—the original *Tallinn Manual on the International Law Applicable to Cyber Warfare*,[17] released in 2013, and the *Tallinn Manual 2.0*, released this spring—are enormous undertakings and incredible achievements. The convener's intent for each, we are told in the *Tallinn 2.0* document itself, was to produce a handbook that would provide an "objective restatement of the *lex lata*" to actual practitioners, primarily "state legal advisers charged with providing international law advice to governmental decision makers, both civilian and military."[18]

I have no doubt that these state actors will indeed find the *Tallinn Manual 2.0* a useful resource. And it will be most useful to these state legal advisers and other practitioners *not* because, as some might assume, it provides flexible, expansive interpretations of the legal rules, which will lend them legal justification for whichever actions they wish to take in cyberspace; rather, it will be useful primarily to the extent it provides them with granular, specific answers regarding their legal obligations and constraints in areas where practitioners may seek clear guidance as to the appropriate legal space in which to operate.

Furthermore, *Tallinn 2.0* does not shy away from areas that might be most controversial for states, such as the role of international human rights law in constraining states' actions in cyberspace. In fact, it tackles this matter

17. *See generally* TALLINN MANUAL, *supra* note 5.

18. TALLINN MANUAL 2.0, *supra* note 5, at 2–3; *see also* Rachel Ansley, *Tallinn Manual 2.0: Defending Cyberspace*, ATLANTIC COUNCIL (Feb. 15, 2017), http://www.atlanticcouncil.org/blogs/new-atlanticist/tallinn-manual-2-0-defending-cyberspace [https://perma.cc/UKC7-3YXG] (quoting Michael Schmitt: "We were not writing for academics. We were writing for countries.").

head-on and announces explicitly that "[i]nternational human rights law is applicable to cyber-related activities."[19] Despite the difficulty in finding consensus among the experts—not to mention the state participants in the process—in determining precisely how specific rules of human rights law operate in cyberspace and the disparity among states in acceptance of particular treaty regimes, the *Manual* firmly states that these rules act as constraints on states.[20] The *Manual* suggests no intent to evade human rights rules; quite the contrary, it suggests (and this is a stated goal of its leadership) an intent to place a marker for future actors to understand that human rights law provides constraints and to prompt them to determine precisely how these rules operate in context.[21]

And yet, despite this clear, human rights-embracing statement and intent, I predict the *Manual* will face some real criticism from the human rights community, and for good reason.[22] The human rights chapter is everything the handbook-style rules regulating state action under the use of force and law of armed conflict (LOAC) sections are not; the legal rules described in the human rights chapter are painted with broad brushstrokes, at a high level of generality, and thus, as I explain below, suggest greater flexibility for state discretion and potentially even evasion. Ultimately, the international human rights law (IHRL) rules laid out by the *Manual* simply provide insufficient clarity to be terribly useful to state legal advisers.

In a vacuum, there may be little danger in a document that simply restates a human rights obligation at a high level of generality. Here, the danger lies largely in the disparity between the human rights chapter and other critical sections of the *Manual*, in particular the significant discussions

---

19. TALLINN MANUAL 2.0, *supra* note 5, at 182 (Rule 34). This statement is consistent with United Nations General Assembly's (UNGA) approach of the last several years. *See, e.g.*, G.A. Res. 68/167, ¶ 3 (Dec. 18, 2013) ("[T]he same rights that people have offline must also be protected online, including the right to privacy.").

20. TALLINN MANUAL 2.0, *supra* note 5, at 182 (Rule 34).

21. *See* TALLINN MANUAL 2.0, *supra* note 5, at 182 (imposing obligation on states to conform to international human rights law in cyberspace despite recognizing that "state understandings concerning the precise scope of certain human rights entitlements in the cyber context . . . vary"); Michael Schmitt, Dir., Tallinn Manual 2.0 Project, Address at the Texas Law Review Symposium: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Feb. 7, 2017). In interviews and writings, *Tallinn*'s director, Michael Schmitt, has explained that the goal of the *Manual* more broadly is to help "states focus their efforts where clarification of the law is needed and in their national interest." *E.g.*, Schmitt, *supra* note 13.

22. The *Manual* is only weeks old, but at least one commentator has raised concerns with its treatment of human rights. *See* Dinah PoKempner, Gen. Counsel, Human Rights Watch, Address at the Texas Law Review Symposium: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Feb. 7, 2017); Dinah PoKempner, *Squinting Through the Pinhole: A Dim View of Human Rights from* Tallinn 2.0, 95 TEXAS L. REV. 1599, 1602 (2017)*; see also* Adams, *supra* note 15.

of the law governing the use of force and LOAC. The *Manual* holds itself out as providing the very clarity and granularity that is missing from the discussion of human rights. And experience suggests that the absence of that specificity may read to states as space or flexibility in the law.

I should include here some caveats. My observations—including that this particular *Manual* is predominantly engaged with the law governing the use of force and LOAC on a level of detail that it does not employ with respect to IHRL—are not intended as criticism of the actors involved here or even of the main approach of the *Manual*. I see two potential reasons for the disparity the *Manual* takes to these two bodies of law: One is actual ambiguity or lack of detail in IHRL and its relationship to cyberspace vis-à-vis LOAC.[23] Another is that the actors involved or the process itself led toward a disparate treatment of these two sections. There may be a bit of each at work here. But these may not be entirely separable factors. Considering the years-long first *Tallinn* process's focus on the rules of cyber *warfare*, we cannot entirely divorce any paucity in the law of human rights in cyberspace from the process's outsized focus on drilling into the laws of war. It may well be that the provenance of the *Tallinn* process gave the laws of war a head start.[24] In any event, as will be clear in my discussion of interpretation catalysts below, I see this disparity as an organic and potentially inevitable development given the original triggers for the project and the path its development has taken. At the end of this section, I will make a modest suggestion for how to address the concerns I raise here. But for now, let us dive into those specific concerns.

First, in order to understand how both state actors and human rights advocates might approach this manual, it is worth understanding some context regarding the relationship of states—in particular the United States—to international human rights law in the realm of conflict and national security. For years, U.S. human rights advocates, in particular, have sought to gain traction with the government on a broad range of matters dealing with conflict and security.[25] And yet there remains a perception—particularly

---

23. *See, e.g.*, Marko Milanovic, *Foreign Surveillance and Human Rights, Part 5: The Substance of an Extraterritorial Right to Privacy*, EJIL: TALK! (Nov. 29, 2013), https://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-5-the-substance-of-an-extraterritorial-right-to-privacy/ [https://perma.cc/6WXQ-XTP2] (discussing the need to "flesh[] out" detailed rules governing an "extraterritorial right to privacy").

24. *See id.* (noting that detailing such rules "will happen in an iterative process").

25. As part of this effort, U.S. human rights organizations have over the course of the last decade and a half created divisions within their institutions specifically devoted to matters of war and national security. *See, e.g.*, *About the ACLU's National Security Project*, AM. CIV. LIBERTIES UNION, https://www.aclu.org/other/about-aclus-national-security-project [https://perma.cc/27CF-4E4U] (detailing the ACLU's "National Security Project," which was "[o]riginally created as an informal working group after the September 2001 attacks"); *see also Counterterrorism*, HUM. RTS.

with respect to the U.S. government—that the law of international human rights has been sidelined in favor of a LOAC framework, LOAC expertise, and even LOAC-derived rules in contexts in which states have struggled to adapt international legal frameworks to new contexts. For example, through three very different presidential administrations, the U.S. government has applied the laws of war to its detention, targeting, and even surveillance operations in the conflict with al Qaeda and other groups.[26] Even when the government has found those rules difficult to map perfectly onto a conflict with a non-state actor, the government has retained a LOAC framework and reasoned by analogy to that body of law in determining the lawful space in which it could operate.[27]

Human rights experts, in the meantime, have repeatedly sought to push the government to accept and apply international human rights norms in this space and to bring U.S. policies in line with these rules.[28] Throughout the

---

FIRST, http://www.humanrightsfirst.org/topics/counterterrorism [https://perma.cc/NA27-KAA4] (highlighting Human Rights First's work at the nexus of national security and human rights); *National Security*, HUM. RTS. WATCH, https://www.hrw.org/united-states/national-security [https://perma.cc/F9C4-3Z8G]; *National Security and Human Rights Campaign*, OPEN SOC'Y FOUND. (Sept. 18, 2013), https://www.opensocietyfoundations.org/grants/national-security-and-human-rights-campaign [https://perma.cc/7VGC-7PYJ]; *Security and Human Rights*, AMNESTY INT'L, http://www.amnestyusa.org/our-work/issues/security-and-human-rights [https://perma.cc/X6N5-G47P] (detailing the work of Amnesty International's U.S.-based affiliate with respect to national security and human rights); *U.S. National Security and Human Rights*, OPEN SOC'Y POL'Y CTR. (Feb. 24, 2017), https://opensocietypolicycenter.org/issues/u-s-national-security-human-rights/ [https://perma.cc/ZN6U-XF5P]

26. Hamdi v. Rumsfeld, 542 U.S. 507, 516 (2004); Respondents' Memorandum Regarding the Government's Detention Authority Relative to the Detainees Held at Guantanamo Bay at 1, *In re* Guantanamo Bay Detainee Litigation, 577 F. Supp. 2d 312 (D.D.C. 2008) (No. 08-442) [hereinafter March 13 Brief]; Rebecca Ingber, *Co-Belligerency*, 42 YALE J. INT'L L. 67, 74–80 (2017). While we do not yet have a definitive statement from the Trump Administration on its legal position on the framework for these conflicts with al Qaeda and other groups, all evidence suggests at a minimum that the Administration intends to continue a wartime framework. *See, e.g.*, Charlie Savage, *ISIS Detainees May Be Held at Guantánamo, Document Shows*, N.Y. TIMES (Feb. 8, 2017), https://www.nytimes.com/2017/02/08/us/politics/guantanamo-islamic-state-detainees.html?_r=0 [https://perma.cc/FBU9-55VW] (discussing a leaked draft executive order announcing the Trump Administration's potential policy of military detention for members of al Qaeda, ISIS, and other groups); Draft Executive Order on Protecting America Through Lawful Detention of Terrorists and Other Designated Enemy Elements (2017), https://assets.documentcloud.org/documents/3455640/Revised-draft-Trump-EO-on-detainees-and-Gitmo.pdf [https://perma.cc/K23D-DXFA] (characterizing, within a leaked draft of a Trump Administration Executive Order obtained by the *New York Times*, conflicts with Al Qaeda and other groups as a "continuing state of armed conflict with terrorist groups").

27. *See* March 13 Brief, *supra* note 26, at 1 ("Principles derived from law-of-war rules governing international armed conflicts, therefore, must inform the interpretation of the detention authority Congress has authorized for the current armed conflict.").

28. *See, e.g.*, Alfred de Zayas, *Human Rights and Indefinite Detention*, 87 INT'L REV. RED CROSS 15, 37 (2005) (rejecting "indefinite detention" as unlawful under international human rights law).

course of the Obama Administration, those efforts of human rights advocates, and the resulting tension with and within the Administration, in addition to pressure from allies, is part of what lay beneath Obama-era attempts to impose an additional layer of often human rights-derived policy prescriptions on top of the Administration's interpretation of its legal constraints on U.S. actions in a range of areas, such as the targeted killing realm.[29] In many of these areas, however, the Obama Administration did not alter those underlying legal positions, which were largely a holdover from the prior Administration's decision to treat the conflict in LOAC terms.[30] As a matter of *law*, the Obama Administration also generally retained a variety of legal tools—including the concept of "*lex specialis*" and the position that many human rights treaties were not intended to apply extraterritorially, both of which I will discuss in more detail below—that together entailed an evasion of a strict application of specific human rights rules onto many of its activities in this space.[31] The result in certain areas was a human rights policy overlay on top of a LOAC legal framework, an outcome Naz Modirzadeh has

29. Press Release, Office of the Press Sec'y, White House, Fact Sheet: U.S. Policy Standards and Procedures for the Use of Force in Counterterrorism Operations Outside the United States and Areas of Active Hostilities (May 23, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/05/23/fact-sheet-us-policy-standards-and-procedures-use-force-counterterrorism [https://perma.cc/Z2BM-VA39] (explaining the policy overlay of procedural safeguards, as well as near-certainty requirements and a preference for capture over kill, for targeting operations).

30. *See* Ashley S. Deeks, *The Obama Administration, International Law, and Executive Minimalism*, 110 AM. J. INT'L L. 646, 646–47 (2016) (arguing that the expansion of power under the Bush Administration enabled the Obama Administration to take a more minimalist approach without sacrificing any of the legal powers gained in the Bush years); Rebecca Ingber, *The Obama War Powers Legacy and the Internal Forces that Entrench Executive Power*, 110 AM. J. INT'L L. 680, 681–82 (2016) (arguing that internal features of the executive branch lead to the retention of legal authorities by the President from one administration to the next).

31. *See, e.g.*, WHITE HOUSE, REPORT ON THE LEGAL AND POLICY FRAMEWORK GUIDING THE UNITED STATES' USE OF MILITARY FORCE AND RELATED NATIONAL SECURITY OPERATIONS 34 (2016), https://www.justsecurity.org/wp-content/uploads/2016/12/framework.Report_Final.pdf [https://perma.cc/R664-YKZE] ("In accordance with the doctrine of *lex specialis*, where these bodies of law conflict, the law of armed conflict would take precedence as the controlling body of law with regard to the conduct of hostilities and the protection of war victims. However, . . . armed conflict does not automatically suspend [o]r . . . displace the application of all international human rights obligations."); Marko Milanovic, *Harold Koh's Legal Opinions on the US Position on the Extraterritorial Application of Human Rights Treaties*, EJIL: TALK! (Mar. 7, 2014), http://www.ejiltalk.org/harold-kohs-legal-opinions-on-the-us-position-on-the-extraterritorial-application-of-human-rights-treaties/ [https://perma.cc/YG99-NTUK] (discussing reports of leaked opinions by then-State Department Legal Adviser Harold Koh advising the U.S. Government to change its position on the extraterritorial application of its ICCPR and CAT obligations); Beth Van Schaack, *United States Report to the UN Human Rights Committee: Lex Specialis and Extraterritoriality*, JUST SECURITY (Oct. 16, 2013), https://www.justsecurity.org/1761/united-states-lex-specialis-extraterritoriality/ [https://perma.cc/R84E-CM44] (laying out the recent history of the U.S. position on *lex specialis* and extraterritoriality of its ICCPR obligations before the Human Rights Committee).

criticized as blurring the lines between genuine legal rules and the policies governing state action.[32] This recent history is an important backdrop against which to examine and understand the *Tallinn Manual 2.0*'s approach to human rights in cyberspace.

The most immediate, and perhaps striking, thing one notes in reviewing the IHRL chapter, particularly in light of the background that I just surveyed, is that its overarching tone is quite friendly to the application of IHRL in cyberspace. The very first rule states firmly and clearly that "[i]nternational human rights law is applicable to cyber-related activities."[33] This written statement accords with the stated intent of the directors of the project, who have noted that their objective in this chapter was to alert state legal advisers of the need to grapple with their state's human rights obligations in this realm.[34] To the extent the simple alerting of legal advisers to the need to address a body of law is the goal, the chapter itself accomplishes this, and perhaps need not have even moved on from that initial rule.

But the chapters of this *Manual* cannot each be read in a vacuum; they exist and will be read alongside the rest of the work as a whole. And when one examines the *Manual* in its entirety, there is a stark contrast between the approach taken in the human rights chapter and that of the other content of the handbook, in particular the nearly 250 pages of direct discussion of LOAC plus additional content threaded throughout the *Manual*. The immediate impression, to say the least, is that human rights law was not the focus of this project.

Now, the fact that a soft law project focuses on one area of law at the expense of or in lieu of another is itself neither an error nor a flaw. Nevertheless, to the extent the project is held out as an overarching manual covering the waterfront on all issues involving cyberspace that may arise for a state, it is important to highlight the contrasting approaches to these different bodies of law and flag some potential hazards, particularly for states looking to this *Manual* as the definitive work on the international law governing cyberspace. In particular, and considering the backdrop I laid out at the start of this section, there are some flags here that suggest state actors might rely upon the human rights chapter as a justification for discretion rather than as a source of clear constraint. I will discuss a few of these here.

---

32. Naz K. Modirzadeh, *Folk International Law: 9/11 Lawyering and the Transformation of the Law of Armed Conflict to Human Rights Policy and Human Rights Law to War Governance*, 5 HARV. NAT'L SECURITY J. 225, 228–30 (2014).

33. TALLINN MANUAL 2.0, *supra* note 5, at 182 (Rule 34).

34. Schmitt, *supra* note 13; *see also* Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEXAS L. REV. 1639, 1640–41 (2017).

### *A. Confinement of the Human Rights Chapter to a Narrowly Defined Geographic Space in the Manual*

One concern with the approach the *Manual* takes to human rights is geographic—both in form and substance. Discussion of human rights in the *Manual* is primarily confined to the human rights chapter—which is itself a relatively short 30 pages in an over 600-page manual, of which about half is devoted to the laws of war.

There are a number of alternative approaches the *Manual* drafters might have taken to address the role of human rights law in this space. A more human rights-focused approach might have been to weave human rights law norms and rules throughout the discussion, in each of the sections, as different scenarios are contemplated, as is done throughout with LOAC.[35] It is not clear to what extent human rights experts who drafted or reviewed the human rights chapter were also involved in the work of the rest of the *Manual* or to what extent they were able to weigh in on each and every rule throughout. But a human rights-driven approach might have resulted in a discussion of how human rights law regulates, for example, how a state may engage civilians who participate in acts of hostilities during armed conflict; or the concept of collective punishment; the rule about cyber booby traps; contemplation of a state's duty to protect cyber infrastructure; or cyber interference with telecommunications; each of which could readily benefit from a discussion of how human rights law also regulates state actions in such circumstances.[36]

Instead, the *Manual* relegates the discussion to a chapter within a larger section marked "specialised regimes," alongside primarily *geographically-focused* legal regimes—like the seas, outer space, and diplomatic premises.[37] Though this was not necessarily intended, a reasonable inference to draw from that placement is that IHRL is a body of law parallel to those specialized regimes. One might be forgiven for assuming that it only exists in some kind

35. *See, e.g.*, TALLINN MANUAL 2.0, *supra* note 5, at 53 (discussing the interplay between jurisdiction, LOAC, and *Tallinn 2.0* Rule 8); *id.* at 74 (discussing how LOAC affects foreign state immunities with respect to *Tallinn 2.0* Rules 44, 82, and 152); *id.* at 127 (discussing the interaction between countermeasures, LOAC, and *Tallinn 2.0* Rules 23, 72, 92, and 113).

36. *Id.* at 217 (discussing the duty to protect cyber infrastructure under Rule 40); *id.* at 288 (discussing the duty to safeguard international telecommunication infrastructure under Rule 61); *id.* at 294 (discussing harmful interference with non-military cyber services under Rule 63); *id.* at 428 (discussing civilian direct participants in hostilities under Rule 97); *id.* at 457 (discussing cyber booby traps under Rule 106); *id.* at 539 (discussing collective punishment under Rule 106). This is not to say the *Tallinn Manual 2.0* is entirely devoid of human rights references outside of that chapter; the *Manual* does include throughout some limited cross-referencing to the human rights chapter, though nowhere near as extensively or fluidly as it interweaves the discussion of LOAC.

37. TALLINN MANUAL 2.0, *supra* note 5, at vi–vii.

of confined geographic space. Of course, the view that a state's human rights law obligations are entirely constrained by geography and inoperative beyond that state's legal borders does exist, and lies on one extreme side of the debate over the extraterritorial application of human rights law. Notably, it is a view that *the Manual itself does not espouse*.[38] Nevertheless, the confined geographic location in the *Manual* seems to reflect a residual sense of human rights law as belonging to a wholly separate and confined space, which belies the complexity of state positions on how they see and apply their obligations outside their borders. And it might help entrench such an impression for state legal advisers relying upon the *Manual* as a guide.

### *B.* Lex Specialis

Another flag for state actors is the *Manual*'s discussion of *lex specialis*.[39] The *Manual* states that the "precise interplay between [LOAC] and [IHRL] remains unsettled," but that under the concept of *lex specialis*, the laws of war will often comprise the more specific rules to apply to armed conflict.[40] There is much packed into that brief statement, and it must be read in light of the context I discussed above, in which—whether there is merit to this approach or not—the concept of *lex specialis* has long been applied by the states to assert formal compliance with human rights law, while evading their specific application to wartime activities. In this case, by not laying out precisely how this rule of *lex specialis* will apply in individual situations, the *Manual* risks suggesting to states that they have significant discretion to disregard human rights rules in armed conflict by pointing to "more specific" LOAC rules. As I will discuss in the section that follows, the *Manual* itself then lays out these LOAC rules in careful detail.

### *C. Lack of Granularity in the Human Rights Rules*

A concern that goes hand in hand with the problem of *lex specialis* is the lack of granularity in the rules announced in the human rights chapter. As I mentioned, this chapter opens with an overarching statement that is quite favorable to the role of human rights in regulating state action. Yet each of

38. *Id.* at 183–87.

39. *Id.* at 181.

40. *Id.* The *Manual* cites for this concept the International Court of Justice Nuclear Weapons advisory opinion, which states that while human rights obligations do not generally "cease in times of war," the interpretation of those obligations is "determined by the applicable *lex specialis*, namely, the law applicable in armed conflict which is designed to regulate the conduct of hostilities." Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226 (July 8).

the rules listed in the chapter is so high-level or vague as to be fairly anodyne in its practical suggestion of constraints on state action.

Consider how the *Manual* might have treated differently even just the substantive areas that it lists under Rule 35, "[i]ndividuals enjoy the same international human rights with respect to cyber-related activities that they otherwise enjoy."[41] Each of these distinct substantive areas, from freedom of expression to privacy to due process, might itself be its own rule, or even its own chapter. This is not for lack of an interest in granularity by the *Manual* itself. Consider the *Manual*'s treatment of any LOAC rule as a comparison. Compare this broad rule, "[i]ndividuals enjoy the same international human rights with respect to cyber-related activities that they otherwise enjoy,"[42] with, for example, Rule 105 prohibiting indiscriminate means or methods:

> It is prohibited to employ means or methods of cyber warfare that are indiscriminate by nature. Means or methods of cyber warfare are indiscriminate by nature when they cannot be: (a) directed at a specific military objective, or (b) limited in their effects as required by the law of armed conflict and consequently are of a nature to strike military objectives and civilians or civilian objects without distinction.[43]

Or Rule 132 on medical computers:

> Computers, computer networks, and data that form an integral part of the operations or administration of medical units and transports must be respected and protected, and in particular may not be made the object of attack.[44]

Or Rule 122 on perfidy:

> In the conduct of hostilities involving cyber operations, it is prohibited to kill or injure an adversary by resort to perfidy. Acts that invite the confidence of an adversary to believe that he or she is entitled to, or is obliged to accord, protection under the law of armed conflict, with intent to betray that confidence, constitute perfidy.[45]

First, the broad human rights rule is phrased as a contingent standard: it is a rule that depends entirely on a state's view of its human rights obligations in other spheres. The LOAC rules, by contrast, are stated as hard prohibitions.

---

41. TALLINN MANUAL 2.0, *supra* note 5, at 187.

42. *Id.* Note that this statement itself was not particularly groundbreaking, considering states have affirmed such a statement through United Nations General Assembly resolutions since 2013. *See, e.g.*, G.A. Res. 68/167, *supra* note 19.

43. TALLINN MANUAL 2.0, *supra* note 5, at 455.

44. *Id.* at 515.

45. *Id.* at 491.

Moreover, the human rights rule operates at a very high level of generality, whereas the LOAC rules are not only noncontingent, they are highly specific. Particularly when viewed alongside such granular LOAC rules, the high level of generality in the human rights chapter may suggest to states that they have significant discretion in how to engage their human rights obligations. For legal advisers who pick up the *Manual* to determine what they need to tell their clients in a particular scenario, these rules may not provide sufficient specificity to be of much use beyond a general notice that there is another potential body of law operating in this realm.

Moreover, the juxtaposition in the *Manual* of highly detailed LOAC rules against a vague, high-level discussion of human rights rules must be considered in light of the *lex specialis* issue I discussed above. Considering the *Manual*'s restatement of the *lex specialis* concept that the more specific rule governs, the *Manual*'s severe disparity in its treatment of human rights law in relation to LOAC rules could easily be read to suggest that the LOAC rules are in fact more "specific" in each case, and thus that they crowd out the IHRL rules, rather than an alternative possibility: that the *Manual* simply did not drill down into—or compel states to develop through the course of two *Manual* processes—each potential principle of human rights law as it applies in the cyber context.

Rather than provide a bona fide handbook on the application of human rights law to cyberspace, this chapter reads as more of a placeholder. The intimation is: international human rights law is real, it is important, and it regulates state action even in this realm . . . and good luck figuring out how to apply it.

### *D. Methodology*

Finally, and perhaps most importantly, even the methodology of the *Manual* itself appears constructed through the lens of use-of-force- and LOAC-based systems of legal rules, and is thus inadvertently weighted against deriving granular rules from human rights law. As the *Manual* explains, the process for adopting rules involved a requirement of consensus among the "International Group of Experts" that a rule reflected customary international law.[46] As such, the rules would be "binding on all states, subject to the possible existence of an exception for persistent objectors."[47] At times, a treaty text might itself "represent[] a reliable and accurate restatement of

46. TALLINN MANUAL 2.0, *supra* note 5, at 4.

47. *Id.*

customary international law,"[48] according to the experts, in which case the *Manual*'s rule will resemble the treaty text.

This approach makes sense in the LOAC context, where state governments largely drive legal interpretation, and where there is a good deal of customary international law, as well as near-universal adoption of many significant treaties such that many are now taken to represent customary international law.[49] That widespread adoption of many treaty regimes and the deep core of customary international law mean that a project to determine the LOAC rules applicable to cyberspace can address a universal set of rules applicable to virtually all states without undermining the entire project.

By contrast, the international human rights legal regime, as Dinah PoKempner addresses in her piece, is heavily treaty-based, and elaborated through a wide array of governmental, quasi-governmental, and even *non*governmental mechanisms.[50] A methodology that is geared toward addressing only those rules that are universally applicable as customary international law or through nearly universally ratified treaties will highly underrepresent the plethora of treaty rules with which any given state is obligated to comply. Likewise, a methodology based solely in rules universally accepted by states misses the disparate array of enforcement mechanisms states face, which play large and differing roles in expounding human rights norms. The *Manual* makes a quick reference to part of this dilemma in the introduction, stating that "[u]sers of this Manual are cautioned that states may be subject to additional rules of international law set forth in treaties to which they are Parties."[51] But the universal and state-driven

48. *Id.*

49. *See, e.g.*, Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 4; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Victims of Non-International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609 (the United States is a signatory of both Additional Protocols but is currently one of very few states which have not yet ratified either); *see also Customary Law*, INT'L COMMITTEE RED CROSS, https://www.icrc.org/en/war-and-law/treaties-customary-law/customary-law [https://perma.cc/26PV-2BTR]. For the long list of treaties applicable to wartime, see *Treaties, States Parties and Commentaries*, INT'L COMMITTEE RED CROSS, https://ihl-databases.icrc.org/ihl [https://perma.cc/2U63-4J8H].

50. PoKempner, *supra* note 22, at 1602 (stating that "nongovernmental experts, practitioners, and scholars have for decades provided much of the 'gas' in the 'engine' of human rights law mechanisms, be they treaty bodies, courts, review conferences, U.N. or regional procedures, or legislatures, and not only through the supply of relevant facts, but through legal analysis and interpretation").

51. TALLINN MANUAL 2.0, *supra* note 5, at 4. Interestingly, the *Manual* does at times point to specific treaty rules of LOAC as applicable to only those states that are party to the treaty. *See, e.g.*, *id.* at 481 (stating under Rule 118, Choice of Targets, "[f]or States Parties to Additional Protocol I,

approach of the *Manual* provides yet another reason for the disparity in granular rules in the human rights section as compared to the rest of the *Manual*.

***

To conclude this section, it is very possible that a simple highlighting of human rights as another set of obligations states will need to address may very well be what the *Manual* drafters intended, or all they felt they could provide, when confronted with an area on which they could not reach consensus, or where there is still much work to do to develop how to apply the law in practice. And from the perspective of those who care about protecting human rights—as I gather the *Manual* experts do—a manual that exhorts its audience to consider human rights law is likely better than a document that ignores it altogether, or much worse, states that this body of law has no place in regulating cyber law. Nevertheless, the *Manual*'s approach to human rights is a far cry from the truly detail-oriented, practitioner-focused handbook that it serves as for other areas of law, particularly for the laws governing the use of force and armed conflict. And that disparity might leave operators with the impression that the rules of international human rights law governing cyberspace truly are undefined and, therefore, highly permissive.

All of this suggests that either human rights law simply was not the focus of this project, or that the experts viewed the state of human rights law as not as well-developed as the rules of LOAC as applied to the cyber realm (or both). If the former, this could be addressed by simply clarifying this early in the *Manual* itself—including front and center in the chapter addressing human rights. Otherwise, the *Manual* risks leaving readers with the impression that the latter—a lack of clarity in the law—is the cause for this disparity.

And if that is the case, if the experts running this process simply found that human rights law as applied to cyberspace was less well-developed than the laws of LOAC, then one has to wonder if that is not itself at least in part a function of the fact that the *Tallinn* project took one path from the start and not another. Considering that this decade-long process has been, after all, a project aimed at developing an understanding of where the law stands, and simultaneously at pushing states to develop that law themselves,[52] the experts leading the first *Tallinn Manual* project on the laws of cyberwarfare could

---

when a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected for cyberattack shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects").

52. *See* Schmitt, *supra* note 13 ("Those who participated in the seven-year Tallinn Manuals' journey hoped only that it would enhance the process of norm identification and elucidation by states.").

rightfully consider themselves to have succeeded if that process in fact compelled states to develop clarity on how LOAC applies in the cyber realm.

As the next section will elaborate, I see the *Manual*'s approach to the human rights chapter as an organic and perhaps inevitable result of the initial trigger for the project itself, which defined the process taken to reach this ultimate result. If this result was driven by the process, the solution cannot easily lie in simply editing or lengthening the chapter itself, or in drilling down more concretely into the human rights rules within the context of the same process. Perhaps the only real option for human rights scholars and practitioners is to take up the task themselves, and draft a human rights-focused manual through a human rights-driven process. For the *Tallinn Manual* itself, however, it would be worth announcing a strong caveat to explain that the methodology, expertise, and direction of the process were not targeted toward the practice and mechanisms of the international human rights legal system, and should not be understood to represent the whole of *lex lata* in that space.

## II. Interpretation Catalysts and Cyber Law

So how did it come to pass that a manual intended to provide clarity for states on rules regulating and constraining their action in cyberspace, may inadvertently provide states with a heightened sense of discretionary flexibility and potentially even—at the most cynical level—tools for evading the application of those rules in the area of international human rights law?

To understand this, we need to consider the context in which the original *Tallinn* process was born, sponsored, drafted, and ultimately published, and then served as the backdrop against which the *Tallinn 2.0* drafters operated.

As I note above, I have written elsewhere that the specific triggers for states' interpretations of the legal rules that bind them have a strong influence on their ultimate legal positions. These "[i]nterpretation catalysts can drive [states] to crystallize a legal view on a matter that is entirely novel; can bring a formerly identified but dormant issue into urgent focus; and can transfer an issue from one decision-making forum to another."[53] Interpretation catalysts influence decision making not only by forcing states to articulate a legal position, but in shaping the process through which states reach that decision, "including by determining a particular question's point of entry within the government, framing the task, shaping the interpretive process, establishing the relative influence of the relevant actors, and informing the contextual pressures and interests that may bear on the decision."[54] For example, the

53. Ingber, *supra* note 3, at 360.

54. *Id.* at 360–61.

state's process for determining its legal position on the rules governing treatment of military detainees might differ dramatically depending on whether the state must first consider its public legal position within the context of drafting briefs in defensive litigation, or instead, in preparation for a hearing before a human rights treaty body.[55] The actors around the decision-making table; the process for reaching a decision; the identities of the actors holding the pen in drafting the specific language as well as the ultimate decider if consensus cannot be reached; the biases; contextual pressures; and time frame against which the decision makers act—all of these factors have a significant influence on the ultimate position the state takes.[56] And all of these factors are driven and defined by the initial "interpretation catalyst" for that decision.

In the case of the *Tallinn* processes, interpretation catalysts have operated on two levels: first, in prompting the creation of and direction for a group of experts seeking to define legal rules as guidance for state actors; and second, in prompting states themselves to participate in and receive guidance from that expert-led process. At the first level, the Estonia cyberattacks not only triggered the initial decision to channel legal decision making into a particular expert-led process; that initial catalyst also defined the creation of the entire process and the context in which the body of experts originated and defined their initial roles. In contrast to the influence of interpretation catalysts on the decision-making processes of a preexisting body, such as a state, the catalyst that triggered the *Tallinn* process could have an even more powerful effect on the resulting decision-making process and positions, because it could influence everything from the ground up, including the constitution and mandate of this new entity.

At the second level, the *Tallinn* processes themselves have functioned as interpretation catalysts, triggering states to engage in legal positioning in response. The *Tallinn* processes have—and have intentionally—impelled states to engage in a rule-definition process on the terms and timing of the *Tallinn* expert-led groups. And those terms and timing included tackling a first-stage, law-of-war-driven project, *Tallinn 1.0*, before taking on the broader process of *Tallinn 2.0*.

### *A. Interpretation Catalysts at Stage One*

Given the significance I place on the initial catalyst for interpretation, a critical—perhaps the most critical—publicly-known piece of this history is the trigger for the *Tallinn* process itself: the cyberattacks on Estonia in 2007,

55. *Id*. at 390.
56. *Id*.

in which large portions of the country's cyber infrastructure—specifically government websites, banks, and Estonian news outlets—were essentially shut down for about three weeks as a result of massive distributed denial of service attacks.[57] These events raised a broad range of legal questions, many domestic, such as how Estonia's penal laws applied to actions in cyberspace, and its rules governing surveillance.

But on the international plane, the governments of Estonia and other states were concerned primarily about questions of state attribution, the range of lawful responses available, and what activities could be or even *must* be taken by Estonia's international allies, including whether Estonia might invoke NATO's Article 5 provisions regarding collective self-defense.[58] Estonia in particular had an incentive to conceive of those events in war terms, considering NATO's mutual defense obligations. For that reason or others, there was a felt need among affected states to understand the legal parameters for how international law rules governing conflict apply in the cyber context, and a pressing need, driven partly by state interest, to understand when and the extent to which such events might rise to the level of a use of force or armed attack. Focusing on how the laws of war in particular might operate in cyberspace was, therefore, partly driven by the reality of external events and partly driven by an interest in viewing those events through that wartime lens. As additional cyberattacks followed worldwide, with relevant states finding themselves on both the defensive and offensive ends of such acts, the need to address a baseline set of rules became apparent.[59]

The first *Tallinn Manual* was born out of this rising awareness about the need to come to terms with how international law regulates state action in the cyber realm. That this first project, *Tallinn 1.0*, focused on cyber *warfare*, and not on cyberattacks that do not meet a use-of-force threshold or on cyber security more broadly, can be traced to this initial trigger for the project. It can be traced to the needs of the Estonian government in particular but also to NATO allies' interests in contemplating their own engagement in those

57. Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007), https://www.wired.com/2007/08/ff-estonia [https://perma.cc/9UL2-98JZ].

58. *See* TALLINN MANUAL 2.0, *supra* note 5, at xxiii (stating, in an introductory note by the current President of Estonia, that the 2007 cyberattacks against Estonia "sped up the establishment of the NATO Cooperative Cyber Defence Centre of Excellence" and that among the center's first activities was to commission the study that became *Tallinn 1.0*); TALLINN MANUAL 1.0, *supra* note 5, at 1 (stating, in a note by Michael Schmitt, that the original *Tallinn Manual* project gathered international law practitioners and scholars in order to "examine how extant legal norms applied to this 'new' form of warfare").

59. *See* TALLINN MANUAL 1.0, *supra* note 5, at 1–2 (discussing the increase in cyber warfare after the 2007 cyberattack on Estonia, specifically citing the 2008 cyberattacks against Georgia and the 2010 "Stuxnet" cyberattack against Iran).

events and to the military nature of the organization that ultimately funded, hosted, and facilitated the process, NATO's Cooperative Cyber Defence Centre of Excellence (CCD COE). The first *Tallinn* process thus collected law-of-war expertise, under the auspices of the CCD COE, in order to seek to define the actual state of the laws of war in cyberspace as they existed at that time.[60]

Following the successful conclusion of the *Tallinn 1.0* process, the project immediately turned toward tackling the broader array of law applicable to peacetime cyber activities. The leaders of the *Tallinn* process recognized that the specific expertise necessary for the first *Tallinn* project on cyber warfare would not be sufficient for the broader scope of *Tallinn 2.0*. Thus, they expanded the team and, while retaining the same leadership, brought in an almost entirely new group of legal experts with backgrounds involving not just the law of armed conflict, but also diplomatic law, the law of the sea, space law, and, as we have discussed, human rights. Moreover, the *Manual* notes that care was taken to send individual chapters out to "experts in the respective subjects" to "prepare[] initial drafts of the rules and commentary," as well as to seek peer review by experts at later points on drafts of the *Manual*.[61]

Yet in broadening the group of experts and expertise—and this is of course only conjecture—the process may have encountered increased friction the second time around in coming to consensus on even what applicable body of law to apply to a particular context, let alone the precise contours of the legal rule. While surely a group of experts in any single field will have areas of disagreement, there are also likely to be significant areas of consensus among actors within a shared field, and more so than there might be if views were instead solicited from a broader array of experts from multiple fields. Thus one can readily imagine that a group of, say, LOAC experts may find more avenues for agreement with respect to how LOAC might apply to a novel context, than would a more diverse group of experts drawn from disparate fields of expertise in seeking consensus on the applicability of rules from any given field. If my instincts are correct, *Tallinn 2.0* was as a whole bound to result in broader brushstroke, less granular rules than *Tallinn 1.0*, based on the simple reality of having to seek agreement and enshrine rules on the basis of the lowest common denominator, in a group of more diverse expertise.

If *Tallinn 2.0* were the whole of the project, a more high-level set of principles than those arising from *Tallinn 1.0* might have been the result of

60. *Id.* at 1; *Manual 2.0 to Be Completed in 2016*, NATO COOP. CYBER DEF. CTR. EXCELLENCE (Oct. 9, 2015), https://ccdcoe.org/tallinn-manual-20-be-completed-2016.html [https://perma.cc/D4TN-DZXU].

61. TALLINN MANUAL 2.0, *supra* note 5, at 6.

the process across the board. Yet the second *Manual* could not escape its ancestry. *Tallinn 2.0* could not but inherit the granular in-the-weeds assessment of LOAC rules as they apply in cyberspace, crafted in the *Tallinn 1.0* process. In updating the *Manual* with a broader group of experts, *Tallinn 2.0* may have updated the LOAC rules, but they and states had been living with the first manual in existence at this point for four years, and the second group of experts would not have seen themselves as having a mandate or need to water them down for the purpose of leveling the playing field with other fields of law in *Tallinn 2.0*. The result—quite possibly the *inevitable* result—is a manual that includes highly granular rules of LOAC, drawn from the first process, alongside more high-level principles applicable in other areas of law.

Were the *Manual* to be read in a vacuum, without an understanding of its history, one would be forgiven for assuming that these other bodies of law are simply less fleshed out, less determinate, in their application to cyberspace. And many of them likely are. Nevertheless, had the process begun with a different focus, not LOAC but a different field of law, it is likely that a homogenous group of experts (and by homogenous I mean in expertise, not in beliefs), in *any* of the fields addressed in the *Manual*, would be better able to reach consensus on the application of their field of expertise to cyberspace than would a body drawn from diverse areas of expertise. And the process itself would have impelled states to consider and develop the application of law in that field, just as the *Tallinn Manual 1.0* authors intended in the LOAC space.

Consider a thought experiment. Imagine that the trigger—the "interpretation catalyst"—prompting experts from Europe and the United States and elsewhere to come together to determine the applicable rules governing cyberspace were not the attacks on Estonia, but instead an event resulting in public and governmental outcry against state surveillance of personal communications. What if the public revelations of Angela Merkel's tapped phone,[62] for example, had instead been the catalyst for this process? At the time of those revelations, states grappled with their response, weighing condemnation of the United States, while simultaneously facing new spotlight on their own surveillance measures.[63] Just as with the use-of-force

62. Mark Mazzetti & David E. Sanger, *Tap on Merkel Provides Peek at Vast Spy Net*, N.Y. TIMES (Oct. 30, 2013), https://nyti.ms/2lqLFPJ [https://perma.cc/N2N8-UEHZ].

63. *See, e.g.*, Michael Crowley, *Spies Like Us: Friends Always Spy on Friends*, TIME (Oct. 31, 2013), http://swampland.time.com/2013/10/31/friends-always-spy-on-friends/ [https://perma.cc/YV34-V4JK] (discussing the prevalence of international spying on allies); Ashley Deeks, *The Increasing State Practice and Opinio Juris on Spying*, LAWFARE (May 6, 2015), https://www.lawfareblog.com/increasing-state-practice-and-opinio-juris-spying [https://perma.cc/BKV2-FGM8] (recalling Germany's reaction to the Snowden revelations in light of the discovery of German surveillance); Melissa Eddy, *Germany Drops Inquiry Into Claims U.S. Tapped Angela*

and law-of-war questions that puzzled states in the aftermath of the Estonia attacks, surveillance too has raised thorny questions regarding the balancing of states' positions on both the offensive and defensive end of such measures.

Had those events instead been the catalyst for this soft law process, we quite likely would have seen a very different group of experts gather to discuss international cyber law, focused primarily on a very different set of core issues.[64] This "Berlin Manual 1.0," as we might have called it, might have focused solely on that initial range of surveillance issues and not attempted to go beyond, just as *Tallinn 1.0* cabined itself to cyber warfare. An entirely different array of experts would have been convened to tackle such issues. They would have taken a methodological approach appropriate to their expertise and to the substantive matter before them. A group of human rights experts, for example, might have started from a perspective of applying treaty rules to cyberspace, rather than starting with customary international law, and might have given more weight to the views of courts, U.N. bodies, and a plethora of other nongovernmental and inter- or quasi-governmental actors.[65] There would have been no shortage of debate about how the rules applied, as surely there was among the law-of-war experts, but a multi-year process would have ultimately yielded some granular set of rules specific to that body of law, and simultaneously pushed the development of the law toward greater specificity as well.

If the "Berlin Manual" were a success, as was *Tallinn 1.0*, we can imagine there would have been clamor for a new manual to cover a broader

---

*Merkel's Phone*, N.Y. TIMES (June 12, 2015), https://nyti.ms/2lebJLy [https://perma.cc/HU3X-8H2X] (describing the German investigation into the allegations and the ultimate withdrawal of the investigation).

64. In the course of the last four years, numerous other processes have in fact been convened worldwide to examine and attempt to define the rules governing cyber activities in a broad range of areas, and these are in various stages of implementation. These include the following: African Union Convention on Cyber Security and Personal Data Protection, June 27, 2014, AU Doc. EX.CL/846(XXV), https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf [https://perma.cc/2DLR-8GQC]; U.N. General Assembly, Letter dated Jan. 9, 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General, U.N. Doc. A/69/723 (Jan. 13, 2015) (introducing the Draft International Code of Conduct for Information Security, authored under the auspices of the Shanghai Cooperation Organization); Organization of American States Res. AG/RES. 2004 (XXXIV-O/04), Appendix A (June 8, 2004), http://www.oas.org/xxxivga/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm [https://perma.cc/6CSR-3UCQ]; High Representative of the Eur. Union for Foreign Affairs & Security Policy, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, JOIN (July 2, 2013), http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf [https://perma.cc/9ACF-Q9UT].

65. *See* PoKempner, *supra* note 22, at 1604 (discussing the myriad state, nonstate, and intergovernmental bodies and mechanisms involved in the interpretation and protection of human rights obligations).

range of issues. The second process, if it were run like *Tallinn 2.0*, would likely take on new members with expertise in particular fields, like LOAC or diplomatic facilities, to take a first cut at their respective chapters. It would likely retain the methodology of the first process, as well as the original set of rules. And then the group as a whole—including that original group of human rights experts—would vote on the new provisions, edit them, determine how best to fit them into the rest of the manual, and perhaps add caveats so that the new chapters in Berlin 2.0 would not undermine the first set of rules they had laid out in Berlin 1.0. I think there is no question that such a process—even assuming the second manual were intended to cover precisely the same body of material as *Tallinn 2.0*, and even were the second group of experts comprising our alternate-universe Berlin 2.0 to be precisely the same people as those who were actually in the room during *Tallinn 2.0*—would yield a very different result.

### *B. Interpretation Catalysts at Stage Two*

The second level at which the interpretation catalyst operates here is the *Tallinn* process itself as an impetus for states to develop cyber law in one particular field. One consistent refrain—in the *Tallinn Manual* itself and from the experts speaking on its behalf—is that the *Manual* is intended to represent the *lex lata* as it stood when the project was drafted and that the drafters did not see it as part of their mandate to push the law in a particular direction.[66] Yet the directors of the project have repeatedly stated their intent to impel states forward in clarifying the law in this space.[67] Moreover, for the reasons I laid out at the start of this section, and in more detail in *Interpretation Catalysts*,[68] the simple existence of such a project, the path of its development, and the reality of its success in drawing the attention of states,[69] has already and will continue to act as a trigger influencing states in their own internal and group decision-making processes. That influence affects state decision making even at an incubatory stage, in the simple act of deciding whether to send an envoy to engage the *Tallinn* process, which specific official to send, from which agency component inside the government, and with what kind of expertise, and in the packaging of talking

66. *See, e.g.*, TALLINN MANUAL 2.0, *supra* note 5, at 3 ("*Tallinn Manual 2.0* is intended as an objective restatement of the *lex lata*. Therefore, the Experts involved in both projects assiduously avoided including statements reflecting *lex ferenda*."); *see also* Schmitt, *supra* note 3; Schmitt & Vihul, *supra* note 34.

67. *See, e.g.*, Schmitt, *supra* note 13 (describing one of *Tallinn 2.0*'s goals as "allow[ing] states to focus their efforts where clarification of the law is needed").

68. Ingber, *supra* note 3, at 360.

69. *See* Schmitt, *supra* note 13 (discussing "The Hague Process"); *Over 50 States Consult Tallinn Manual 2.0*, NATO COOP. CYBER DEF. CTR. OF EXCELLENCE (Feb. 2, 2017), https://ccdcoe.org/over-50-states-consult-tallinn-manual-20.html [https://perma.cc/3QKS-W3Y7].

points the state puts together for that expert to deliver. The original *Tallinn* process's focus on the laws of war is inextricably intertwined with a concomitant need for states to engage with that process through their own law-of-war experts and resources. Should states then drive the law forward in the cyberwarfare realm, the experts leading the *Tallinn 1.0* process would rightfully mark that legal development a success, but we cannot ignore that this development must occur at the opportunity cost of a focus on other bodies of law that might subsequently be left less defined in the cyber realm.

### *C. Harnessing the Power of Interpretation Catalysts*

This case study illustrates not only the power of interpretation catalysts in driving the direction of law as it develops, but also how such triggers can be harnessed, even manipulated, as a means of influencing the path that development takes. As I have noted, the initial Estonia cyber attacks, and the response to them, need not have been conceived primarily in war terms. In fact, the *Tallinn Manual* itself ultimately concluded both that "the law of armed conflict did not apply to those cyber operations because the situation did not rise to the level of an armed conflict," and that "there is no definitive evidence that the hacktivists involved in the cyber operations against Estonia in 2007 operated pursuant to instructions from any State, nor did any State endorse and adopt the conduct."[70] The resulting *Tallinn* project itself might thus have focused primarily on nonwartime legal questions, such as the prohibition on intervention, and indeed, on human rights law. Yet, as I noted above, there were incentives for state actors seeking to create this process to conceive of those events in war terms,[71] and that conception, in turn, may have enabled greater interest from state allies and prompted NATO engagement. In any event, whatever the impetus for that conception, these attacks, the atmospherics and language of "warfare" that surrounded them, the concomitant establishment of the NATO Cooperative Cyber Defence Centre of Excellence, and its immediate commissioning of the *Tallinn* study on cyber warfare, all determined the subsequent path for the development of the law in this space.

## Conclusion

Doctrinal debates about the appropriate legal rules to apply to novel contexts at times mask institutional undercurrents that led to the adoption or

70. TALLINN MANUAL 2.0, *supra* note 5, at 376, 382.

71. *See id.* at xxiii (stating, in an introductory note by the current President of Estonia, that the 2007 cyberattacks against Estonia marked "the first time one could apply the Clausewitzean dictum: War is the continuation of policy by other means").

interpretation of any particular rule. The initial triggers for the development of a legal position, and the institutional reality of the decision-making process that plays out, may have an enormous influence on the path that process takes and the resulting decision. Yet debates about doctrine do not typically address these triggers or the institutional process taken as a result.[72]

In concluding, it is worth considering some of the benefits inherent in a soft law process initially driven by law-of-war expertise and discipline. There is inherent in law-of-war-driven processes a focus on practical, operational rules and on how to employ them. There is a focus on states and what states will be willing to accept and implement, as well as useful—and to some degree unique—levels of engagement between scholars and practitioners working in this realm. The combination of practicality and engagement gives these experts added legitimacy in seeking to constrain state actors. And finally, at the broadest level, law-of-war experts are a group of individuals who have cut their teeth applying laws to space that others tend to see as lawless. That willingness to regulate what others may view as ungovernable is particularly important for an endeavor seeking to determine the rules applicable in cyberspace.

Considerations of institutions, actors, and process are critical when grappling with the development of law, and they are necessary to our consideration of the differing substantive bodies of law addressed in the *Tallinn Manual 2.0*. As the *Manual*'s directors have acknowledged, the discussion of human rights was a significant challenge for this project.[73] It has met with some criticism, and it may very well meet with more, particularly the more states rely upon it.[74] Debate will likely center on the specifics of the doctrinal rules, how the *Manual* grapples with those rules, and the difficulties in deriving clear legal guidance for states in this realm. But when considering those critiques, and the extent to which the *Manual* does or does not sufficiently drill down into any particular body of law, it is essential to contemplate the origins and path of the development of this project. The status of cyberlaw as it exists today is, and will continue to be, inextricably bound up in the initial approach taken to the events that triggered its development.

---

72. For a compelling account of how the evolution of the EU's human rights engagement turned on early, "pragmatic" decisions of the founding Member States, see Grainne De Burca, *The Road Not Taken: The EU as a Global Human Rights Actor*, 105 AM. J. INT'L L. 649 (2011).

73. *See* TALLINN MANUAL 2.0, *supra* note 5, at 4 (acknowledging the *Manual*'s limitation in the field of human rights law); Schmitt, *supra* note 13; *Tallinn Manual 2.0 to Be Completed in 2016*, NATO COOP. CYBER DEF. CTR. EXCELLENCE (Oct. 9, 2015), https://ccdcoe.org/tallinn-manual-20-be-completed-2016.html [https://perma.cc/VER5-QW7T] (quoting managing editor Liis Vihul as stating, "During this session, the most difficult material proved to be international human rights law governing activities in cyberspace.").

74. *See, e.g.*, *supra* Part I; PoKempner, *supra* note 22, at 1599.