Tallinn Manual on the International Law Applicable to Cyber Warfare. Edited by Michael N. Schmitt. Cambridge, New York: Cambridge University Press, 2013. Pp. xix, 282. Index. $120, cloth; $58.99, paper.

In 2009, the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) in Tallinn, Estonia, invited a group of independent experts—the International Group of Experts (IGE)—on the law of armed conflict to produce a manual on cyber warfare. The drafters, led by Michael N. Schmitt, who chairs the international law department at the U.S. Naval War College, included a mix of well-regarded practitioners, academics, and technical experts, as well as observers from NATO's Allied Command Transformation, U.S. Cyber Command, and the International Committee of the Red Cross. Over the course of several years, the IGE developed the *Tallinn Manual on the International Law Applicable to Cyber Warfare*. The *Tallinn Manual* provides a thorough and careful analysis of how the *jus ad bellum* and *jus in bello* translate to cyberspace, along with helpful descriptions of divisive issues that remain to be resolved through state practice and debate. Although the *Tallinn Manual*'s reliance on the Western and NATO-centric perspectives of its drafters may hamper its acceptance in countries, such as China and Russia, that espouse very different visions for cyberspace, the *Tallinn Manual* offers an indispensable resource for scholars, practitioners, and policy makers.

The *Tallinn Manual* is designed to provide "some degree of clarity to the complex legal issues surrounding cyber operations" (p. 3) and, in particular, to describe "the applicable *lex lata*, that is, the law currently governing cyber conflict," not "*lex ferenda*, best practice, or preferred policy" (p. 5). The *Tallinn Manual* styles itself as a cyberwar incarnation of earlier nongovernmental codification or restatement efforts, including the *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*[1] and the *Manual on International Law Applicable to Air and Missile Warfare*.[2] The introduction describes the *Tallinn Manual* as the product of an "expert-driven process designed to produce a non-binding document applying existing law to cyber warfare" (p. 1), and it takes pains to note that the *Tallinn Manual* is neither a NATO document, despite the sponsorship of the NATO CCD COE, nor a reflection of the official position of any state or organization from which the experts are drawn.

Following an introduction by Schmitt describing the project and its genesis, the *Tallinn Manual* sets out ninety-five black-letter rules and accompanying commentary. Rules in part I address *jus ad bellum* issues, such as sovereignty, state responsibility, the prohibition on the use of force, and self-defense, while rules in part II cover *jus in bello* issues, such as permissible targets, proportionality, occupation, and neutrality. Each rule was adopted by consensus among the IGE and is intended to "replicate customary international law" (p. 6), unless otherwise noted. Although the *Tallinn Manual* itself is a nonbinding document, it explains that to the extent the rules "accurately articulate customary international law, they are binding on all States, subject to the possible existence of an exception for persistent objectors" (*id.*).

The *Tallinn Manual*'s ambitious scope and broad coverage of the *jus ad bellum* and *jus in bello* reflect a strong degree of agreement among the IGE. The agreement on specific rules builds on the IGE's consensus about a more foundational aspect of international law applicable to cyberwar, namely the IGE members' unanimous agreement that "general principles of international law appl[y] to cyberspace" and rejection of the idea that "international law is silent on cyberspace in the sense that it is a new domain subject to international legal regulation only on the basis of new treaty law" (p. 13).[3]

[1] SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA (Louise Doswald-Beck ed., 1995).

[2] PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH AT HARVARD UNIVERSITY, MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE (2009), *available at* http://www.ihlresearch.org/amw/manual.

[3] The *Tallinn Manual* further notes: "Despite the novelty of cyber operations and the absence of specific rules within the law of armed conflict explicitly dealing with them, the International Group of Experts was

While the rules on which the IGE agreed are very useful in advancing thought and debate about international law regarding cyberwar, more valuable still are the instances in which the *Tallinn Manual* frankly acknowledges disagreement within the IGE. The commentary to many rules notes majority and minority positions on particular issues or applications of the rules and sometimes simply indicates that the IGE is not unanimous. Predictably, rules about which disagreements arose include some of the most debated legal issues in the *jus ad bellum* and *jus in bello* and the most difficult factual scenarios related to cyberwar.

In some instances, the lack of agreement stemmed from cyber-specific difficulties. For example, the IGE disagreed about whether a cyber operation that causes "extensive negative effects," but does not "result in injury, death, damage or destruction," could constitute an armed attack (p. 56). The paradigmatic example of such an operation is an action directed at a major stock exchange. Some members of the IGE argued that physical injury to persons or property is a requirement for an armed attack, while others "emphasized the catastrophic effects such a crash would occasion and therefore regarded them as sufficient to characterize the cyber operation as an armed attack" (*id.*).

Another cyber-specific disagreement arose over a state's placement of malware on the cyber infrastructure of another state. The IGE agreed that a state's cyber operation that causes *damage* to the cyber infrastructure of another state violates the second state's sovereignty, but could not reach consensus on whether "the placement of malware that causes no physical damage (as with malware used to monitor activities) constitutes a violation of sovereignty" (p. 16).

A further disagreement centered on the application of Rule 5 on "[c]ontrol of cyber infrastructure" (p. 26). The rule declares that "[a] State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States" (*id.*). While the rule's application to acts that a state discovers while such acts are in progress is clear, the rule's application to *prospective* acts divided the IGE. Some IGE members argued that a state has an affirmative duty to "take reasonable measures" to prevent its cyber infrastructure from impacting other states, but others took the opposite approach, arguing that "no duty of prevention exists, particularly not in the cyber context given the difficulty of mounting comprehensive and effective defences against all possible threats" (p. 27). The knowledge requirement for Rule 5 also split the IGE. Specifically, disagreement arose regarding whether constructive knowledge suffices to create an obligation on the part of the state. In other words, does a state violate the rule if it "fails to use due care in policing cyber activities on its territory and is therefore unaware of the acts in question"? (p. 28).[4] Consistent with its disclaimer that the *Tallinn Manual* simply assesses the law as it is and does not proffer policy and law that might be desirable, the commentary does not grapple with the implications for privacy or private-network ownership of requiring a state to monitor and police the cyber activities occurring on its cyber infrastructure or within its territory.

Other disagreements represent the cyber analogue to well-worn controversies in the *jus ad bellum* and *jus in bello*. For example, the *Tallinn Manual* declares that "[n]o international cyber incidents have, as of 2012, been unambiguously and publicly characterized by the international community as reaching the threshold of an armed attack" (p. 57). The IGE disagreed, however, about the point at which a use of force constitutes an armed attack, including in the particular application of those designations to the reported U.S. and Israeli Stuxnet operations against Iranian nuclear facilities. The *Tallinn Manual* takes the position that deployment of the Stuxnet worm constituted a use of force (p. 45),[5] but only some

unanimous in finding that the law of armed conflict applies to such activities in both international and non-international armed conflicts . . . ." (p. 75).

[4] Further disagreement among the IGE exists regarding the rule's applicability to states through which a cyber operation is routed, in addition to the state from which an operation originates (pp. 28–29).

[5] The *Tallinn Manual* states in the commentary to Rule 10 on the "[p]rohibition of threat or use of force," that the "clearest cases are those cyber operations, such

IGE members, citing the damage caused to Iranian nuclear centrifuges, believe that Stuxnet also reached the threshold for constituting an armed attack (p. 58).

Another disagreement that the *Tallinn Manual* carries over into the cyber context from conventional warfare relates to the permissibility of anticipatory self-defense. Rule 15 on "[i]mminence and immediacy" specifies that "[t]he right to use force in self-defence arises if a cyber armed attack occurs or is imminent. It is further subject to a requirement of immediacy" (p. 63). The commentary to Rule 15 explains that a majority of the IGE believe that although Article 51 of the UN Charter does not "expressly provide for defensive action in anticipation of an armed attack, a State need not wait idly as the enemy prepares to attack" and "may defend itself once the armed attack is 'imminent'" (*id.*). As a factual matter, determining the imminence of a cyber attack may be more challenging than detecting an imminent conventional attack. Neither satellite imagery that can show missiles being positioned nor radar that can reveal incoming aircraft will warn of an imminent cyber attack. Nonetheless, the legal dispute about the permissibility and lawful extent of anticipatory self-defense under Article 51 of the UN Charter is an old dispute with a new incarnation, not a new legal question.

As these descriptions make clear, the *Tallinn Manual* provides a helpful and detailed distillation of how existing law applies in the cyber context. The *Tallinn Manual* is a superb resource for those interested in cyber law of war issues, and it provides an excellent complement to recent academic work focused more narrowly on particular questions. As the first broad exposition of laws of war as related to cyber issues, the *Tallinn Manual* will likely serve as a focal point for debates going forward, with scholars and other experts turning to the *Tallinn Manual* as a point of departure for thinking and writing about cyber law of war questions.

It remains to be seen, however, whether or how the *Tallinn Manual* will impact the actors with which it is primarily concerned: states. The *Tallinn Manual* is an important contribution, at least in part, because "State cyber practice and publicly available expressions of *opinio juris* are sparse" (p. 5). The secrecy surrounding states' actions in cyberspace poses a challenge for any attempt, like the *Tallinn Manual*, to distill customary international law. Moreover, for both state practice that has come to light and governmental actions that have not been publicly revealed, governments have undoubtedly developed legal analyses to address some of the same issues that the *Tallinn Manual* covers. States have begun to explain publicly some of their legal reasoning on the most fundamental questions,[6] but states engaged in or contemplating cyber actions likely have completed more detailed analyses that are not public. For governments that have already undertaken extensive analysis, the *Tallinn Manual* may not cover new analytical ground, but the comprehensive scope of the *Tallinn Manual*'s coverage and the experience of its drafters may prompt even such governments to consult the *Tallinn Manual* as a useful resource.

Beyond the question of whether states qua states will embrace the *Tallinn Manual*, a broader challenge is whether non-NATO states, experts, and commentators will agree in substance with the *Tallinn Manual* or be willing to rely on it. The drafting process may have inadvertently hampered the prospects for broad geographic acceptance of the resulting product. All of the *Tallinn Manual*'s drafters, technical experts, and observers hail from

as the employment of the Stuxnet worm, that amount to a use of force" (p. 45).

[6] For analysis from the United States, see, for example, U.S. National Security Council, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World 10, 14 (May 2011), *at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [hereinafter U.S. International Strategy for Cyberspace]; Harold Hongju Koh, *International Law in Cyberspace: Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012*, 54 HARV. INT'L L.J. ONLINE 1 (2012), *at* http://www.harvardilj.org/2012/12/online_54_koh; Advance Questions for Vice Admiral Michael S. Rogers, USN Nominee for Commander, U.S. Cyber Command, Mar. 11, 2014, at 11–12, *at* http://www.armed-services.senate.gov/download/rogers_03-11-14 (discussing U.S. military's evaluation of use of force and self-defense with respect to cyber actions).

the United States, Western Europe, or Australia (pp. x–xii). The same is true of those who served as peer reviewers. Moreover, the selection of national military manuals from Canada, Germany, the United Kingdom, and the United States as reference materials does nothing to dispel the perception that the *Tallinn Manual* is channeling, even though not officially representing, a particular worldview with respect to the laws of armed conflict (p. 8).[7] The *Tallinn Manual* is careful to note that the use of these four national manuals "should not be interpreted as a comment on the quality of any other such manuals," but it also explains that IGE members participated in drafting each of the four national manuals, thus reinforcing the perception that the national manuals confirm, rather than diversify, the perspectives reflected in the *Tallinn Manual* (*id.*). At a minimum, it would be helpful to know whether the manuals of other states address or diverge from the positions reflected in the *Tallinn Manual*.

The lack of geographic diversity among the *Tallinn Manual*'s drafters casts some doubt on the value of the *Tallinn Manual*'s statements about the breadth of the views reflected. As noted above, the *Tallinn Manual* explains that the IGE "assiduously sought to capture all reasonable positions for inclusion" in the commentary and "to articulate all competing views fully and fairly for consideration by users of the Manual" (pp. 6–7). The positions captured, however, are those of experts from particular geographic regions.

Similarly, statements about the IGE's unanimity, such as that the group was "unanimous in its estimation that both the *jus ad bellum* and *jus in bello* apply to cyber operations" (p. 5), may not reflect worldwide unanimity on such issues. For example, at the time the *Tallinn Manual* was published in April 2013, it was not clear that China, a major power in the cyber domain, believed that any existing law applied to cyberspace.[8] In June 2013, China's position became somewhat clearer when, in the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, it joined consensus on the basic principle that "[i]nternational law, and in particular the Charter of the United Nations," applies in cyberspace.[9] China's past reluctance to acknowledge the application of even the UN Charter, along with its broader disagreement with the United States and its allies about the role of sovereignty in cyberspace,[10] suggests that it may have substantive, doctrinal differences from the perspectives reflected in the *Tallinn Manual*. The *Tallinn Manual*, however, does not address whether or how China's assessments of the *jus ad bellum* and *jus in bello* might differ from those agreed upon by the IGE. Achieving true worldwide agreement at the present time would be a tall and quite likely impossible order. But avoiding cyber conflict and escalation of cyber incidents will ultimately require common global understandings about the boundaries of acceptable and unacceptable actions in cyberspace.

[7] By way of explanation, the *Tallinn Manual* notes that these four national manuals are "publicly available" (p. 8). However, other studies have consulted and cited a broader range of national military manuals. For example, the study by the International Committee of the Red Cross on customary international humanitarian law used military manuals as evidence of state practice and cites military manuals from, inter alia, Cameroon, Colombia, Israel, Kenya, Nigeria, and Russia. 1 JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, INT'L COMM. OF THE RED CROSS, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW xxxii, 4 n.9, 8 n.40 (2005).

[8] *See, e.g.*, OFFICE OF THE SECRETARY OF DEFENSE, ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA 2013, at 36 (May 2013), *at* http://www.defense.gov/pubs/2013_china_report_final.pdf ("Although China has not yet agreed with the U.S. position that existing mechanisms, such as international humanitarian law, apply in cyberspace, Beijing's thinking continues to evolve.").

[9] Report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, para. 19, UN Doc. A/68/98* (July 30, 2013); *see id.* at 12–13 (annex listing the members of the UN Group of Governmental Experts).

[10] *Compare* U.S. International Strategy for Cyberspace, *supra* note 6, at 22 (advocating a multistakeholder governance model), *with* Ministry of Foreign Affairs of the People's Republic of China, *China, Russia, and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations*, para. 7 (Sept. 13, 2011), *at* http://nz.chineseembassy.org/eng/zgyw/t858978.htm (promoting multilateral governance model).

Although other perspectives may emerge to challenge the *Tallinn Manual*'s legal conclusions, for scholars and others focused on cyberwar issues the *Tallinn Manual* is now the go-to resource on the law applicable to cyberwar. Because of the *Tallinn Manual*'s focus on cyber warfare and the breadth of legal issues encompassed by that topic, its drafters excluded from the project "[c]yber activities that occur below the level of a 'use of force' (as this term is understood in the *jus ad bellum*), like cyber criminality" (p. 4). At least some below-the-threshold issues, however, will be addressed by the upcoming NATO CCD COE's "Tallinn 2.0" project. Tallinn 2.0 will tackle issues including the law of state responsibility, law of the sea, and international telecommunications law, as well as explore in greater depth certain principles, such as sovereignty and the prohibition on intervention, that the *Tallinn Manual* (or Tallinn 1.0) briefly addresses.[11] The project, scheduled for completion in 2016, will provide guidance for the below-the-threshold actions and legal issues that are as important as and more frequent than the cyberwar questions covered in Tallinn 1.0. The expanded coverage of Tallinn 2.0 will be a welcome addition to the important contribution the *Tallinn Manual* has made to the debates about law and cyberwar.

KRISTEN E. EICHENSEHR
UCLA School of Law

Privatizing War: Private Military and Security Companies Under Public International Law. By Lindsey Cameron and Vincent Chetail. Cambridge, New York: Cambridge University Press, 2013. Pp. xxxv, 720. Index. $150.

It is by now no surprise to learn that the use of private military and security companies (PMSCs) is a widespread phenomenon. Over the last two decades, such contractors have been deployed by governments in war zones and hot spots around the globe, and their numbers often surpass those of uniformed military personnel.[1] Nevertheless, the legal frameworks applicable to these contractors are still somewhat of a mystery. Although breathless accounts of contractors operating in law-free zones are hyperbolic, the uneven overlapping patchwork of domestic and international laws that regulate these contractors' behavior is riddled with holes and remains poorly understood.

In *Privatizing War: Private Military and Security Companies Under Public International Law*, Lindsey Cameron of the University of Geneva and Vincent Chetail of the Graduate Institute of International and Development Studies, Geneva, have done a heroic job of imposing some analytic order on this seeming legal chaos, at least with respect to public international law. Bringing great rigor, depth, and clarity to the task, the authors provide a systematic overview of the multiple bodies of public international law that govern the contractors themselves and the states and others that employ them. At more than seven hundred pages, the book is not an easy read, but it is breathtaking both in its scope and attention to detail and will surely serve as a lasting and essential resource for anyone working in the field of privatized foreign affairs.

Nevertheless, because the book is so focused on applying formal international law principles to contractors, it largely misses an opportunity to grapple with how such principles are most likely to be enforced in actual practice or to rethink how international law enforcement in general might operate in an era of privatization. The authors spend the vast bulk of this massive book parsing the international law rules to determine under what circumstances a court or tribunal might determine that a PMSC is violating international law, but they devote only scant attention to alternative modes of accountability that have a far greater chance of being effective in implementing the principles and values of international human rights and humanitarian law. Such alternative modes of accountability include mobilizing greater domestic contract law and compliance

[11] *See* NATO CCD COE, Tallinn 2.0 (undated), *at* http://www.ccdcoe.org/tallinn-20.html.

[1] COMM'N ON WARTIME CONTRACTING IN IRAQ AND AFGHANISTAN, TRANSFORMING WARTIME CONTRACTING: CONTROLLING COSTS, REDUCING RISKS—FINAL REPORT TO CONGRESS 18 (2011), *available at* http://cybercemetery.unt.edu/archive/cwc/20110929213815/http://www.wartimecontracting.gov.