Maurer School of Law: Indiana University
Digital Repository @ Maurer Law

Articles by Maurer Faculty | Faculty Scholarship

2015

Technology and the Law on the Use of Force: New Security Challnges in the Twenty-First Century, by Jackson Maogoto

Asaf Lubin

Follow this and additional works at: https://www.repository.law.indiana.edu/facpub

 Part of the International Law Commons, Military, War, and Peace Commons, and the Science and Technology Law Commons

LAW LIBRARY
INDIANA UNIVERSITY
Maurer School of Law
Bloomington

prosecution that took shape after World War II (p. 298). However, Lewis's own account of the wars makes it seem that the fundamental difference was power and state interests: the Allies of World War II had more *power* than the Allies of World War I, and could therefore impose tribunals on the defeated.[20] By the same token, a mainstream explanation for the creation of the ICC is the power shift that occurred after the Cold War.[21]

In *Prologue to Nuremberg*, James Willis acknowledged the difficulty of drawing a clean causal arrow from World War I to Nuremberg. He concluded, "whatever lasting significance the effort to punish the war criminals of the First World War may have remains uncertain. . . . It was the prologue of a revolutionary development in international law, and like other revolutions it emerged from varied influences and motives."[22] Lewis has taken the final chapter of Willis's work and turned it into a book of remarkable detail. In it, he makes an admirable effort to trace the development of international criminal law from 1919 to 1950, accounting for many causes. But that history still appears to be a Gordian knot. Lewis shows us that the knot is complicated, but he does not quite manage to untie it. He does not prove that all the strings of his narrative matter or that they can be united. Perhaps this is an impossible task and he does it as well as anyone could. But it is ultimately a bit unsatisfying. And, perhaps, this is why so many realists try to slice through the knot with one simple answer: the self-interest of states.

Technology and the Law on the Use of Force: New Security Challnges in the Twenty-First Century. By Jackson Maogoto. Oxford, UK: Routledge, 2015. Pp xviii, 111. Price: $117.71 (Hardcover). Reviewed by Asaf Lubin.

In *Technology and the Law on the Use of Force*, Dr. Jackson Maogoto sketches the legal challenges to the regime on the use of force in the digital age. The author is particularly concerned with how technological advances within the "Information Revolution" in military affairs challenge current international legal regulation.[23] As part of this revolution, militaries are gravitating towards heavier reliance on non-kinetic uses of force (i.e. the ability to create effects that do not rely on physical explosives or munitions) in the conduct of their

20. In contrast with the unconditional surrender and zones of occupation after World War II, the Allied victors of World War I could not even obtain extraditions. For instance, the Dutch, supported by the Vatican and other neutral powers, refused to extradite the ex-Kaiser. The Germans also refused to extradite military officials, instead conducting their own (dubious) trials in Leipzig (pp. 55-59).

21. *See* WILLIAM A. SCHABAS, AN INTRODUCTION TO THE INTERNATIONAL CRIMINAL COURT ix-x (4th ed. 2011).

22. *See* JAMES F. WILLIS, PROLOGUE TO NUREMBERG: THE POLITICS AND DIPLOMACY OF PUNISHING WAR CRIMINALS OF THE FIRST WORLD WAR 176 (1982). Lewis himself appears to agree, listing the end of the Cold War first among a "confluence of factors" that made way for the ICC (p. 283).

23. *See* Norman C. Davis, *An Information-Based Revolution in Military Affairs*, *in* IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE 79, 79 (John Arquilla & David Ronfeldt eds., 1997) (noting as early as 1997 that as a result of advances in computerized information and telecommunications technologies, the world "is on the cusp of an epochal shift from an industrial- to an information-based society," which is bound to fundamentally change the way war is conducted).

operations. With governments' critical infrastructures becoming increasingly dependent on digital systems and information technologies, two new domains for military offensive interferences have emerged: the "fourth domain" of outer space, and the "fifth domain" of cyberspace (pp. 23-27). The author examines these domains at great length throughout the book, and attempts to show how "hi-tech weaponry" has so far been regulated by "low-tech legal safeguards" (Chapter Two). Maogoto's book, in this regard, adds to the expanding literature calling for a new international legal order to govern new types of non-armed coercive interventions, including in the form of information warfare (p. 86).[24]

The book comprises five short chapters. Chapter One reviews the doctrines and principles identified under the U.N. Charter's regime governing *jus ad bellum*. As part of the chapter, the author posits restrictionist against counter-restrictionist approaches to the U.N. Charter to tease out the "shades of legal grey" that surround the prohibition on the use of force and the inherent right of legitimate self-defense as articulated by the Charter's drafters (pp. 13-14).

Chapter Two focuses on the problems posed by military technology in the twenty-first century. The militarization and weaponization of outer space and cyberspace strains traditional definitions of the use of force regime (a concept that is introduced in Chapter One). Maogoto argues that while technology has leapt ahead, the legal framework has failed to adapt, rendering states unable to effectively defend themselves against these new types of threats (pp. 27-29).

Chapters Three and Four provide case studies on outer space and cyberspace, respectively. The chapters reflect upon some of the most troubling questions for scholars writing in this field. For example, what do the terms "peaceful purposes," "threat" and "use" of force, "armed attack," and "self-defense" entail in a world of military communication satellites and wired infantries? Would the manipulation of another state's satellite into a different orbit be considered a violation of U.N. Charter Article 2(4), and how should we treat electronic blockades or the destruction of data using malware in cyberspace?

Chapter Five rounds up the discussion with forward-looking evaluations of current international legal principles' ability to constrain potential hostile action in the outer and cyberspace domains. The author seeks to "disengage legal shadows from operational substance" (pp. 72-76),[25] i.e. to restate the law, as a first step towards a reorientation of the international peace and security

24. *See, e.g.*, BATTLEFIELD OF THE FUTURE: 21ST CENTURY WARFARE ISSUES (Barry R. Schneider & Lawrence E. Grinter eds., 1998); Emily Haslam, *Information Warfare: Technological Changes and International Law*, 5 J. CONFLICT & SECURITY L. 157 (2000); Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023 (2007); Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L L. 825 (2001); Michael N. Schmitt, *Computer Network Attacks and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1999).

25. In a way, this methodological approach resembles that of Professor W. Michael Reisman, which determines the status of a particular sub-field in international law by examining the discrepancies between its "myth system" and its "operational code." *See* W. MICHAEL REISMAN, FOLDED LIES: BRIBERY, CRUSADES, AND REFORMS 34-35 (1979).

framework. In particular, the author puts forward two potential prescriptive models: (a) a moratorium (and eventually a total ban) on the deployment of weapons in outer space (p. 78); and (b) the development of a conclusive multilateral framework for cyberspace that would both refocus the principle of nonintervention, and reconceptualize the legal threshold for information warfare (pp. 83-85).

The book provides an abbreviated summary of the legal discourse concerning the use of force and information warfare in the twenty-first century. This concise analysis, which is important in and of itself, is perhaps the book's greatest contribution to the scholarship in this field. However, the book might disappoint those hoping to find novel operative recommendations and suggestions for international legal regulation moving forward. Aside from making general observations, Chapter Five does not detail the contents of either a suggested moratorium or ban in the outer space domain or a potential governing multilateral framework in the cyberspace context.

In reading Maogoto's book, one cannot help but be reminded of Professor Colin Picker's article entitled *A View from 40,000 Feet: International Law and the Invisible Hand of Technology*.[26] In this article, Picker suggests that "technology is an invisible hand guiding, destroying, and creating international law."[27] As noted by some commentators writing on information warfare technologies as early as 1998, "no law can change as swiftly as technology; unless law is to somehow stop technology's seemingly inexorable worldwide progress, it cannot fully control the use of its fruits for warfare. Legal measures can thus supplement, but not supplant, vigilance, preparedness, and ingenuity."[28] In many respects, Maogoto's reliance on legal regulation as a panacea seems almost anachronistic given the supremacy and inevitability of technological advancement.

In addition to these concerns, the book does not adequately address the topic of espionage. At certain junctures, Maogoto seems to suggest, without further explanation, that "passive" surveillance (from either outer space or cyberspace), when serving minimum order goals, would be legitimate. For example, Maogoto suggests that passive outer space surveillance by states for the detection of nuclear explosives on earth, serves "peaceful purposes," and would thus be deemed lawful (p. 72). But the question of the lawfulness of the "second-oldest profession" under international law is an unresolved one.[29] In

26. Colin B. Picker, *A View from 40,000 Feet: International Law and the Invisible Hand of Technology*, 23 CARDOZO L. REV. 149 (2001).

27. *Id.* at 202.

28. LAWRENCE T. GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW 37 (1998).

29. Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071, 1129-30 (2006) (suggesting that until effective political and legal mechanisms are developed, "intelligence will continue to exist in a legal penumbra, lying at the margins of diverse legal regimes and at the edge of international legitimacy"); *see also* Richard A. Falk, *Foreword* to ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW, at v, v (Ronald J. Stanger ed., 1962) ("[T]raditional international law is remarkably oblivious to the peacetime practice of espionage. Leading treatises overlook espionage altogether or contain a perfunctory paragraph that defines a spy and describes his hapless fate upon capture"); W. Hays Parks, *The International Law of Intelligence Collection*, *in* NATIONAL SECURITY LAW 433, 433-34 (John Norton Moore et al., eds., 1990) ("No

light of the fact that, as part of the information revolution, the function of intelligence collection in cyberspace and outer space has significantly intensified, one would expect Maogoto to have discussed it further in the development of his thesis.

Finally, it would seem that Maogoto conveniently dodges the legal and factual complexities posed by the increasing privatization of both the outer space and cyberspace domains. The author makes clear at the outset that his research focuses "only on those information intrusions that are instigated by or imputable to States," suggesting that as a matter of general practice "non-statal activity" tends to fall within the spectrum of criminal law rather than the use of force paradigm (p. 5). However, the author himself recognizes the difficulty in establishing a sufficient nexus for the purposes of attribution of wrongful conduct to states in these domains (referencing, for example, the difficulty in ascribing liability to States in the context of the "Code Red" and "Stuxnet" worms). Moreover, individuals are becoming even more active than certain states in operating within the digital global commons; consider, for example, George Clooney's involvement with the Satellite Sentinel Project,[30] or the international network of "hack-tivists" known as Anonymous.[31] The erosion in the power of states, as they lose their monopoly over the fourth and fifth domains, leads to an accountability gap that Maogoto unfortunately avoids.

Regardless of these few shortcomings, *Technology and the Law on the Use of Force* provides valuable observations for scholars and policy makers interested in the field of information and security. Maogoto neatly charts out, in a short and powerful book, a complete list of the pitfalls of currently existing regulatory frameworks governing the fourth and fifth domains. Readers should expect to find more questions than answers, as Maogoto only provides a call for action by defining the areas within the law in need of further clarification. It is up to international practitioners to shed light on the legal shadows and penumbras of information warfare in the *jus ad bellum.*

---

serious proposal ever has been made within the international community to prohibit intelligence collection as a violation of international law because of the tacit acknowledgment by nations that it is important to all, and practiced by each"); Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 321 (1996) ("International Law regarding peacetime espionage is virtually unstated, and thus, international law has been an inappropriate and inadequate reference for either condemnation or justification of actions involving intelligence gathering.").

30. *See generally* Chris Rojek, *'Big Citizen' Celanthropy and its Discontents*, 17 INT'L J. CULT. STUD. 127, 134 (2013) (further detailing Clooney's involvement with the Harvard Sentinel Project to surveil human rights abuses in South Sudan).

31. *See generally* Noah C.N. Hampson, *Hacktivism: A New Breed of Protest in a Networked World*, 35 B.C. INT'L & COMP. L. REV. 511 (2012) (analyzing the phenomenon of hacktivism from an international law perspective).