INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1901
U.S. NAVAL WAR COLLEGE

The Road Ahead: Gaps, Leaks and Drips

Michael J. Glennon

89 INT'L L. STUD. 362 (2013)

Volume 89 2013

The Road Ahead: Gaps, Leaks and Drips

Michael J. Glennon[*]

I. INTRODUCTION

Might there be gaps in the international rules governing cyber conflict, and if so, are they likely to be filled? Is this the right way to think about these questions?

Whether gaps exist in international law seems at first to be a technical, almost marginal issue. On analysis, however, the question[1] emerges as one

---

* Professor of International Law, Fletcher School of Law and Diplomacy, Tufts University. This paper draws upon *The Dark Future of Cyber-Security Regulation*, 6 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 563 (2012). I thank Beau Barnes for research assistance and Cecile Aptel, William Banks, Robert Barnidge, Toni Chayes, Matt Hoisington, Peter Margulies, Michael Matheson, Vijay Padmanabhan, Alexandra Perina, Robert Sloane, Gary Solis and Cecilia Vogel for comments on an earlier draft. Errors and views are my own.

1. The literature on the broader question of lacunae and *non liquets* in international law is neither new nor thin. *See* MALCOLM N. SHAW, INTERNATIONAL LAW 92–93 (5th ed. 2003); Daniel Bodansky, Non Liquet *and the Incompleteness of International Law*, *in* INTERNATIONAL LAW, THE INTERNATIONAL COURT OF JUSTICE AND NUCLEAR WEAPONS 153 (Laurence Boisson de Chazournes & Philippe Sands eds., 1999); Ole Spiermann, Lotus *and the Double Structure of International Legal Argument*, *in id.* at 131; Prosper Weil, *"The Court Cannot Conclude Definitively . . .":* Non Liquet *Revisited*, 36 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 109 (1997); Julius Stone, Non Liquet *and the Function of Law in the International*

that goes to the very "source of validity of international law," rather in the manner that questions posed by quantum mechanics go to the heart of the physical structure of the universe.[2] Nowhere are the issues more urgent or far-reaching than in the realm of cyber war.

Press reports about Stuxnet[3] and related activities suggest the unease with which cyber activities fit within the framework of existing rules. Was "Olympic Games," the covert operation in which Stuxnet was employed, a use of force within Article 2(4) of the United Nations Charter? Did Olympic Games constitute an "armed attack" under Article 51—which would have permitted defensive use of force by Iran against the United States and Israel? Is this an international armed conflict governed by international humanitarian law? Is the United States unlawfully using civilians in combat—or are the persons at the keyboards combatants because they are directly participating in hostilities? If so, who are the combatants? The Central Intelligence Agency's computer staff? The officer who pushed the "enter" button? Does it matter whether they fail to "carry arms openly" or wear a "fixed distinctive sign recognizable at a distance"?[4] Can they be prosecuted if they're captured by Iran, or extradited to Iran by a friendly State?[5]

Community, 35 BRITISH YEARBOOK OF INTERNATIONAL LAW 124 (1959); Hersch Lauterpacht, *Some Observations on the Prohibition of "*Non Liquet" *and the Completeness of the Law*, *in* SYMBOLAE VERZIJL 196 (Marinus Mijhoff ed., 1958), *reprinted in* 2 HERSCH LAUTERPACHT, INTERNATIONAL LAW: COLLECTED PAPERS OF HERSCH LAUTERPACHT 213 (Elihu Lauterpacht ed., 1975); John Dickinson, *The Problem of the Unprovided Case,* UNIVERSITY OF PENNSYLVANIA LAW REVIEW 115 (1932).

2. *See* Stone, *supra* note 1, at 125.

3. *See, e.g.*, David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, NEW YORK TIMES, June 1, 2012, at A1.

4. *See* Convention Relative to the Treatment of Prisoners of War art. 2, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Prisoners of War Convention].

5. Similar questions arise in connection with drone strikes. *See* Gary Solis, *America's Unlawful Combatants*, WASHINGTON POST, Mar. 12, 2010, at A17. For thoughtful consideration of whether gaps exist in the rules governing detention during conflicts with non-State groups, see John B. Bellinger III & Vijay M. Padmanabhan, *Detention Operations in Contemporary Conflicts: Four Challenges for the Geneva Conventions and Other Existing Law,* 105 AMERICAN JOURNAL OF INTERNATIONAL LAW 201 (2011).

II. THE ILLUSION OF COMPLETENESS

Some of the articles in this volume and much general commentary[6] suggest that the *jus ad bellum* and *jus in bello* rules that might address such questions contain no gaps. The assumption appears to be that the rules are comprehensive, comprising categories like squares on a huge juridical quilt that covers every possible fact situation and leaves no legal question unanswered. The implication is that only one correct answer exists for every such question,[7] since a complete system would leave no room for multiple, equally correct, conflicting answers to the same question. Finding the correct answer is merely a matter of accurate classification: identify the characteristics of the activity in question, and then place it neatly within the appropriate legal category. That there exist gray areas on the margins of each category makes classification more difficult but does not defeat it. The right answer is out there, waiting to be discovered, embedded in "community values,"[8] earlier rules,[9] their overarching purposes or some other juridically endogenous source that transcends humanity's fleeting differences. Good lawyers everywhere ultimately will come to the same correct conclusion as to how ambiguities should be resolved and which category is the right one. The analytic process is thus a logical sequence of binary choices: something like Stuxnet is either a use of force or not a use of force, an attack or not an attack, armed or not armed, perpetrated by combatants or noncombatants, and so on. Categories like these have a clear core; if judges can identify that core, the rest of us can as well. Find it, make the right choice at each step,

---

6. For representative recent writings, see TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., forthcoming 2013), draft *available at* http://issuu.com/nato_ccd_coe/docs/tallinn_manual_draft/1#share.

7. For an argument along these lines, see "Judge Hercules'" ability to identify the one right answer in RONALD DWORKIN, LAW'S EMPIRE 239 (1986) ("I must try to exhibit [the] complex structure of legal interpretation, and I shall use for that purpose an imaginary judge of superhuman intellectual power and patience who accepts law as integrity. Call him Hercules.").

8. Community-values adherents typically flesh out the concept with reliance upon notions such as security, human dignity, social progress, quality of life and self-determination. *Cf.* Dickinson, *supra* note 1, at 128 (referring to "the idea that all the materials which enter into the construction of a new legal rule for an unprovided case must themselves be law").

9. *See id.* at 118 ("The notion that legal rules are so connected rationally that one can be deduced from others leads to the conclusion that in the last analysis there is no such thing as an unprovided case. . . . [T]he law for new cases is to be found inside the law itself and not by resort to considerations and ideas drawn from outside the field of technical law.").

work through an idealized, neatly deduced decision tree and a single, accurate conclusion will appear.

This view has obvious attractions. It eliminates the specter of a "legal vacuum" from which, it is supposed, believers in the rule of law ought naturally to recoil. It promises a Holy Grail of universality, the glimmering possibility that good intentions and assiduous effort will yield unanimity. It eradicates analytic confusion by giving every legal problem a crystalline answer. It provides emotional succor to those who seek refuge from the bewildering tangle of conflicting wants, needs and emotions that spring from cultural, political and philosophical differences. It removes the perilous possibility that a non-existent gap in the law might be claimed by waterboarders and their ilk as a pretext for violation. It gives judges an airtight rationale for deciding every case without trenching upon legislative or sovereign prerogatives, as the case may be, since adjudication always entails interpreting existing rules rather than making new ones. It counters the growing problem of fragmentation in the international system. And it eliminates the frustrating need to come to consensus on new rules: if no gaps need be filled, no new rules need be devised. For lawyers puzzling over the rules that govern cyber war, cyber attacks, cyber defense and the like, this view of law is beguiling.

It has but one drawback—it doesn't deliver on its promises.

It's the wrong way to think about international law generally and the wrong way to think about the law of armed conflict in particular. The approach has been rejected by the International Court of Justice (ICJ)[10] and dismissed by legal scholars for over a hundred years as arid formalism, legal fundamentalism, noble dreams, mechanical jurisprudence, mythmaking and various other pejoratives[11]—for understandable reasons.

---

10. *See infra* notes 34–35.

11. In Germany, formalism was critiqued by Philip Heck and other proponents of a "jurisprudence of interests." *See* Philip Heck, *The Jurisprudence of Interests: An Outline*, *in* THE JURISPRUDENCE OF INTERESTS 31 (M. Magdalena Schoch ed. & trans., 1948). In France, François Gény argued that formal legal sources were inadequate to address all legal questions. *See* FRANÇOIS GÉNY, MÉTHODE D'INTERPRÉTATION ET SOURCES EN DROIT PRIVÉ POSITIF (La. State Law Inst. trans., 1963); Richard Groshut, *The Free Scientific Search of François Gény*, 17 AMERICAN JOURNAL OF JURISPRUDENCE 14 (1972). In the United States, legal realists pressed for greater attention to the consequences that categories produced, suggesting the propriety of "rule skepticism" and "fact skepticism" in the classification process. *See* JEROME FRANK, COURTS ON TRIAL: MYTH AND REALITY IN AMERICAN JUSTICE (1949); Hans Kelsen, *The Pure Theory of Law: Its Method and Fundamental Concepts*, 50

Think back to the earliest years, the years in which the law of armed conflict was young and rules were few. Did these pioneering, stand-alone rules leave no gaps? The few early rules were isolated patches; the "quilt" of international humanitarian law, such as it is, emerged only gradually, over many years.[12] In the initial years of the law's development, numerous matters that were later to be addressed by the rules remained uncovered.[13] At what point in the law's evolution did it become all-encompassing, leaving no question unanswered, like the rules of chess? At what point did human imagination freeze, losing all capacity to exploit ambiguities in the existing rules? When, precisely, did the law's development end? With the Hague Convention of 1899,[14] or 1907?[15] With the four 1949 Geneva Conventions?[16] With the additional protocols of 1979?[17] When did the system become complete? How would we know if it were complete?

At regular historical intervals, of course, general, prophylactic principles (such as the Martens clause, discussed later) did emerge, the ultimate import of which was undifferentiated humanitarianism. Unless one takes some form of moral intuition as transforming itself inexorably into legal

---

LAW QUARTERLY REVIEW 474 (1934); Roscoe Pound, *The Ideal Element in American Judicial Decision*, 45 HARVARD LAW REVIEW 136 (1931).

12. *See generally* JOHN FABIAN WITT, LINCOLN'S CODE: THE LAWS OF WAR IN AMERICAN HISTORY (2012); *see also* GARY B. SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR 3–10 (2010).

13. *See* Dickinson, *supra* note 1, at 116 ("In the seventeenth and the early part of the eighteenth century, when many of the lines of our present legal processes were laid down, it is fair to say that the problem of the unprovided case was taken for granted and not clearly envisaged as a problem at all.").

14. Convention with Respect to the Laws and Customs of War on Land, July 29, 1899, 32 Stat. 1803.

15. Convention No. IV Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2227.

16. Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Prisoners of War Convention, *supra* note 4; 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.

17 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609.

rules,[18] however, precepts that mandate unspecified altruism can hardly be considered sufficient to obviate the need for additional, more particularized squares on the legalist quilt, such as, for example, prohibitions against the use of dumdum bullets or noxious gases. These specific prohibitions and myriad others like them were considered necessary precisely because generalized exhortations to good conduct left room for reasonable disagreement as to what was expected. No evidence exists to suggest that the law has arrived—or ever will arrive—at some millennial zenith beyond which no further refinement need be contemplated. Evolving human wants, needs and emotions will continue to produce the ever-changing mishmash of clashing, culturally variant preferences from which international law flows.[19]

Nor, for that matter, is there any reason to believe that further legalization would necessarily be a good thing. Concerns about "law-free zones" take as the starting point that legal regulation is better than no legal regulation. But this is not always true; whether a "legal vacuum" is desirable depends upon the alternative and the law's effects. African captives on a nineteenth-century slave ship would not likely have hailed international law's prohibition against visitation of the vessel and release of its human cargo as filling a welcome gap in customary rules governing the slave trade.[20] It is not self-evident that a rule classifying Stuxnet as an armed attack ultimately would promote international peace or security. Compared with the alterna-

---

18. For a comment on Michael Walzer's effort to apply his notion of "practical morality" to war, see Michael J. Glennon, *Pre-empting Proliferation: International Law, Morality, and Nuclear Weapons*, 23 EUROPEAN JOURNAL OF INTERNATIONAL LAW ___ (forthcoming 2012). Though much of the formalism that pervades international humanitarian law can be attributed to surviving ghosts of a naturalist worldview, additional forces are at play, including the influence in Europe of a civil law tradition with purportedly comprehensive codes, and, in the United States, the continued emphasis on appellate cases in legal education, implying no need to examine exogenous, contextual sources to predict case outcomes. *See* Karl N. Llewellyn, *Some Realism About Realism—Responding to Dean Pound*, 44 HARVARD LAW REVIEW 1222 (1931). The oft-repeated claim that "we are all realists now" has yet to embrace all within international law's "invisible college."

19. Prosper Weil put it well:

> Regardless of the judicial and scholarly endeavors to affirm the completeness of international law, the truth of the matter is that international law is not complete. No legal order is, because there is not, cannot be, and should not be a rule at hand for every concrete or new situation. . . . More than municipal law, international law is by its very nature riddled with gaps.

Weil, *supra* note 1, at 118.

20. *See* The Antelope, 23 U.S. (10 Wheat.) 66 (1825). *See generally* Jean Allain, *Nineteenth Century Law of the Sea and the British Abolition of the Slave Trade,* 78 BRITISH YEARBOOK OF INTERNATIONAL LAW 342 (2007).

tive of airstrikes, Stuxnet probably was cheaper and more effective, risked no casualties, might have averted a major war, and—at least until its sponsorship was leaked—set no untoward precedent. Would that legal regulation could always do so well: less, in the legal realm, sometimes is more.

Consider closely the analogical process involved in classifying Stuxnet and other cyber weapons and it becomes apparent that categorization involves much more subjectivity than the formalists suggest. The circumstances that led to an old rule's creation can be similar in some respects to current circumstances but different in others; which elements take priority? There exists no objective standard by which to identify the characteristics of an act or thing that are salient for classification purposes, or how much weight one characteristic is to be given relative to another, or the level of generality or particularity with which they are to be stated, or whether instrumentalities or effects are dispositive.[21] One often can pull the accordion

---

21. NATO States have consistently argued, for example, that the UN Charter limits only harm caused by traditional instrumentalities—weapons—rather than cutoffs of foreign aid, trade boycotts, economic sanctions or other activities that might have the same consequences as an armed attack. Matthew Waxman has concisely summarized the traditional understanding:

> The dominant view in the United States and among its major allies has long been that the Article 2(4) prohibition of force and the complementary Article 51 right of self-defense apply to military attacks or armed violence. The plain meaning of the text supports this view, as do other structural aspects of the U.N. Charter. For example, the Charter's preamble sets out the goal that "armed force . . . not be used save in the common interest." Similarly, Articles 41 and 42 authorize, respectively, the Security Council to take actions not involving armed force and, should those measures be inadequate, to escalate to armed force. Moreover, Article 51 speaks of self-defense against "armed" attacks. There are textual counter-arguments, such as that Article 51's more specific limit to "armed attacks" suggests that drafters envisioned prohibited "force" as a broader category not limited to particular methods. However, the discussions of means throughout the Charter and the document's negotiating history strongly suggest the drafters' intention to regulate armed force differently and more strictly than other coercive instruments. This interpretation has generally prevailed over alternatives. . . .

Matthew Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4),* 36 YALE JOURNAL OF INTERNATIONAL LAW 421, 427–28 (2011) (footnotes omitted). *See also* Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK LAW REVIEW 1023, 1040–42 (2007). The State Department Legal Adviser, however, has indicated that "if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force." Harold Hongju Koh, Remarks at the U.S. Cyber Command Inter-Agency Legal Conference: International Law in Cyberspace (Sept. 18, 2012), http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/. Why actual physical damage should be required to bring an activity within the scope of Article 2(4) of the Charter is not clear; an ineffectual, attempted attack em-

of analogy wide or push it tightly together without risk of being proven wrong.[22] Much the same can be said of efforts to establish the law's completeness and continuousness through reliance upon supposed community values and underlying purposes. The assertion that community values concerning use of force are "shared" is belied by extensive international opinion polling,[23] as well as State practice and *opinio juris*.[24] To the extent that consensus does exist, it must be formulated at so high a level of generality and embrace so many different values, policies and political preferences as to support multiple, equally compelling and sometimes conflicting conclusions. These can be overcome only by presupposing an international consensus that does not now exist and never did exist.[25] Thus formalist analysis easily becomes outcome oriented, producing, in the words of Hersch Lauterpacht, a "deceptive clarity":

> [A]pparent indecision [by the International Court of Justice] . . . may—both as a matter of development of the law and as a guide to action—be preferable to a deceptive clarity which fails to give an indication of the inherent complexities of the issue.
>
> In so far as the decisions of the Court are an expression of existing international law—whether customary or conventional—they cannot but reflect the occasional obscurity or inconclusiveness of a defective legal system.[26]

---

ploying chemical or biological agents would seemingly constitute a use of force notwithstanding the absence of physical consequences. If the physical consequences of economic sanctions or trade boycotts cause physical damage, ought they too to be considered a use of force?

22. For discussion of the levels-of-generality problem in customary law, see MICHAEL J. GLENNON, LIMITS OF LAW, PREROGATIVES OF POWER: INTERVENTIONISM AFTER KOSOVO 50–52 (2001).

23. *See* Glennon, *supra* note 18.

24. *See generally* GLENNON, *supra* note 22.

25. Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command: Before the S. Armed Services Comm., 111th Cong. 11 (Apr. 15, 2010), http://www.armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf ("There is no international consensus on a precise definition of a use of force, in or out of cyberspace. Consequently, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force."). *Compare* Koh, *supra* note 21.

26. HERSCH LAUTERPACHT, THE DEVELOPMENT OF INTERNATIONAL LAW BY THE INTERNATIONAL COURT 152 (1982).

False claims of clarity aimed at concealing the obscurity and inconclusiveness of legal rules that might or might not apply to hard cases generate only incoherence. What make hard cases hard is their incommensurability and our inability to devise objective criteria that render them commensurable.[27] In fact, as Hart wrote, "[s]uch cases are not merely 'hard cases'"; the problem is that "the law in such cases is fundamentally *incomplete*: it provides *no* answer to the questions at issue in such cases."[28]

Some insist that, because legal categories have a clear core, the international legal system is not "defective" at all and that ostensible gaps disappear. Even assuming that the category in question does have a clear core, however, it is ambiguity *at the margins* that produces gaps—gaps that disappear only if it's assumed that every ambiguity is in the end spurious and has a single, correct resolution, or that nothing but law goes into the making and interpretation of law, or that a relevant, pre-existing rule always twinkles like some far-off star exerting emanations from a penumbra that light up the one correct answer. Yet how, again, do we know this? Sometimes the galaxy seems empty; other times the galaxy seems to contain equally radiant stars. The formalists present no standard to assess which star is brighter, insisting only that one *must* be brighter and that reasonable people *must* come to the same, unfalsifiable outcome. But legal rules are not like stars. They don't emit luminosity that can be measured.[29] We have only the naked eye to judge their proximity. Rules are made up, created by human beings. Sometimes, but not always, they're given a specified priority as against other rules, as in the case of constitutional rules versus statutes. But even then, the nearest rules can be so remote in time, subject, or specificity as to generate honest doubt about their applicability.[30] Conflicts can arise

27. *See* John Finnis, *On Reason and Authority in* Law's Empire, 6 LAW AND PHILOSOPHY 357 (1987).

28. H.L.A. HART, THE CONCEPT OF LAW 252 (2d ed. 1997) (emphases in original).

29. For the suggestion that normativity exists in gradations, see Prosper Weil, *Towards Relative Normativity in International Law?*, 77 AMERICAN JOURNAL OF INTERNATIONAL LAW 413 (1983).

30. General, elastic norms are sometimes considered principles rather than rules. Rules are more specific, less malleable and cover less. Rules were described by Pound as "precepts attaching a definite detailed legal consequence to a definite, detailed state of facts." Roscoe Pound, *Hierarchy of Sources and Forms in Different Systems of Law*, 7 TULANE LAW REVIEW 475, 482 (1933). Principles, in contrast, are more general and constitute "authoritative starting points for legal reasoning, employed continually and legitimately where cases are not covered or are not fully or obviously covered by rules in the narrower sense." *Id.* at 483. Pound thus regarded principles as "hortatory." Roscoe Pound, *For the "Minority Report,"* 27 AMERICAN BAR ASSOCIATION JOURNAL 664, 677 (1941). Holmes, too, was

among rules of the same priority, efforts to reconcile the rules can fail, reasonable disagreement can arise as to which prevails, and a court can fairly resolve the controversy either way[31]—or can decline to resolve the controversy at all in the belief that its writ does not extend to rulemaking. The word that describes such a situation is *gap*.

Nor is it an answer to say that gaps don't exist because judges fill the gaps. Whether gaps exist and whether judges should fill them are different questions. Of course judges *can* sometimes fill the gaps; whether they *may* do so depends upon the authority given them by the specific legal system in which they sit.[32] When the law yields no answer, judges not infrequently find themselves asked, in effect, to decide on the basis of personal politics or philosophy[33]—as they declined to do in the *Nuclear Weapons* advisory opinion, where the ICJ (not for the first time)[34] acknowledged a gap of ex-

---

skeptical of their utility. When on the Supreme Court, he invited his fellow justices to name any legal principle on which they relied, suggesting that he could show them how it could be used to decide the case under consideration either way. *See* LOUIS MENAND, THE METAPHYSICAL CLUB: A STORY OF IDEAS IN AMERICA 340 (2004). Principles concerning the meaning of sovereignty, such as the sovereign equality of States, non-intervention and related concepts, do cover gaps and might presage future cyber rules, but they're not concrete enough to resolve categorization problems that flow from rules, and some principles have been ignored so often by so many States that their vitality is questionable. Non-intervention is an example. *See* Peter Ackerman & Michael J. Glennon, *Building Liberty: The Right Side of the Law,* AMERICAN INTEREST (Sept.–Oct. 2007), http://www.the-american-interest.com/article.cfm?piece=313; GLENNON, *supra* note 22.

31. *See generally* JOSEPH RAZ, BETWEEN AUTHORITY AND INTERPRETATION: ON THE THEORY OF LAW AND PRACTICAL REASON 11 (2009) ("[W]e cannot expect the law of any one country to have a uniform way of demarcating the boundary between what belongs to it and what lies outside of it, let alone expect to find that all legal systems demarcate the boundary in the same way.").

32. The Supreme Court appeared to identify the point at which indeterminacy pushes law interpreting into lawmaking in the seminal political question case of *Baker v. Carr*, 369 U.S. 186 (1962), where it found itself barred from deciding a question that involved "a lack of judicially discoverable and manageable standards for resolving it; or the impossibility of deciding without an initial policy determination of a kind clearly for nonjudicial discretion. . . ." *Id.* at 217. Such questions are non-justiciable, it seems, because a gap in the law precludes their resolution.

33. "In these cases it is clear," H.L.A. Hart wrote, "that the rule-making authority must exercise discretion, and there is no possibility of treating the question raised by the various cases as if there were one uniquely correct answer to be found, as distinct from an answer which is a reasonable compromise between many conflicting interests." HART, *supra* note 28, at 132.

34. See, for example, *Barcelona Traction, Light & Power Co., Ltd.* (Belg. v. Spain) (Second Phase), 1970 I.C.J. 3, 33–34 (Feb. 5), in which the ICJ found that "international law has

actly the sort here at issue.[35] Some legal systems are hospitable to judges' making up rules in such circumstances;[36] others are not.[37] Legal systems draw different lines between law interpreting and law creating. Some judges acknowledge the distinction; others do not.[38] In any event, in the first instance and sometimes in the last—before the judges intervene, and when judges won't intervene—lawyers must look to their own judgment to advise

---

not established its own rules" concerning "the rights of states with regard to the treatment of companies and shareholders"; *Haya de la Torre* (Colom. v. Peru), 1951 I.C.J. 71, 80 (June 13), in which the Court stated that the applicable law did not "give a complete answer" to the asylum question at issue; and *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), 1986 I.C.J. 14, 135 (June 27), in which the Court, addressing the question whether international law placed restrictions on a State's military arsenal, declared that "in international law there are no rules, other than such rules as may be accepted by the State concerned, by treaty or otherwise, whereby the level of armaments of a sovereign State can be limited."

35. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 105(2)(E) (July 8). The specific issue on which the Court was unable to reach a conclusion concerned whether the threat or use of nuclear weapons would be lawful or unlawful in an extreme circumstance of self-defense, in which the very survival of a State would be at stake. Judge Vereshchetin wrote separately that in an advisory proceeding that presents such a lacuna, the Court "ought merely to state this" and "cannot be blamed for indecisiveness or evasiveness where the law . . . is itself inconclusive." *Id.* at 280. Judge Higgins, on the other hand, wrote separately to emphasize that applicable norms "indubitably exist" and that "the judge's role is precisely to decide which of two or more competing norms is applicable in the particular circumstances." *Id.* at 592.

36. *See generally* Stone, *supra* note 1. In *Banco Nacional De Cuba v. Sabbatino*, 376 U.S. 398 (1964), the United States Supreme Court was urged to decide the case on the merits because, it was argued, "United States courts could make a significant contribution to the growth of international law, a contribution whose importance, it is said, would be magnified by the relative paucity of decisional law by international bodies." *Id.* at 434. The Court declined the invitation. "[G]iven the fluidity of present world conditions," it concluded, "the effectiveness of such a patchwork approach toward the formulation of an acceptable body of law concerning State responsibility for expropriations is, to say the least, highly conjectural." *Id.*

37. It is notable that the jurisdictional grant of the International Court of Justice directs it not to decide all disputes as are submitted to it, but "to decide *in accordance with international law* such disputes as are submitted to it" (Statute of the International Court of Justice art. 38(1), June 26, 1945, 59 Stat. 1055, 33 U.N.T.S. 993 (emphasis added)), suggesting that a gap in international law would require judicial abstention.

38. One ought to be skeptical, Hart urged, about "ritual language used by judges" who claim to be "the mere 'mouthpiece' of the law which [they] do not make or mold." HART, *supra* note 28, at 274. Prominent jurists such as Holmes, Cardozo and respected Law Lords have recognized that there are "cases left incompletely regulated by the law," cases in which judges have an "inescapable" lawmaking task, and that "many cases could be decided either way." *Id.*

clients, and lawmakers must look to their own judgment to decide whether existing rules are adequate.[39] The rejoinder that a single correct answer awaits them, if only they have the wits to find it, is a conclusion, not an argument—and it is moreover a conclusion that, again, defies falsification (for no counterexample can be hypothesized that could show that no such answer exists).

All this applies with particular force to international law. International law does not present a neat sequence of straightforward binary choices between "A" and "Not A." Junctures that the formalists regard as forks along the way in fact present a third choice: *neither* "A" *nor* "Not A." The third choice is "*No law*." At these junctures, the category in question doesn't seem quite right, but rejecting that category doesn't seem entirely right either. These are questions on which the law is either non-existent or unclear, but the result is the same: reasonable people can differ.

Contrary to the formalists' fears, however, acknowledging ambiguity doesn't open the door to a law-free zone, because international law applies a default rule in such circumstances. Its default rule is the famous freedom principle, from the *Lotus* case.[40] The principle has it that in the absence of a rule a State is deemed free to act, and that a burden of persuasion falls upon the State that alleges some limitation or restriction on another State's freedom of action. The formalists are, perversely, in this sense right that there are no gaps in the international legal order; what would otherwise be a gap is filled with the rule that a State is free to act unless some other State has shown that the acting State has consented to a restriction or limitation on its freedom of action. This possibility of a third option in resolving a dispute concerning the applicability of a category is more than a kind of

---

39. Keeping the rules alive by adding more fine print, judicially or legislatively, may seem at first blush like moving toward a more complete system with fewer ambiguities. In fact, more rules can lead to more gaps, not fewer, as when the law specifies new categories to which rules apply but says nothing about categories *not* specified, implying *expressio unius est exclusio alterius*.

40. The words of the Permanent Court of International Justice in *Lotus* are worth recalling:

> International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot therefore be presumed.

S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, ¶ 44 (Sept. 7).

juridical afterthought, invented for dealing with legal uncertainty. The third option, the freedom principle, is an affirmation of State sovereignty that encapsulates the foundational architecture of the international legal order.

The *Lotus*'*s* notion that the system is wholly consent based is, in the end, simplistic, in the sense that the international legal order is hardly devoid of coercion. The system does not rest upon pure, unfettered consent by all within it; policymakers within States often do things that they don't want to do and refrain from doing things that they do want to do. Other States, international organizations, non-governmental organizations and influential national elites all exercise various forms of power; all narrow States' ability to choose freely. The difference between the international legal system and domestic legal systems lies, rather, in the immediacy, source, extent and consequences of coercion, and the structure of incentives or disincentives that results. If the notion of consent that the international order pictures is taken as a form of constructive rather than actual consent, however, the freedom principle provides a useful shorthand that emphasizes basic structural differences.[41]

Whatever the conceptual difficulties with the notion of consent, it remains true that unless a restriction is established, a State remains free to act. Universalists dislike the notion that anything not prohibited is permitted, for holding out as it does the ever-present possibility that a State might defeat universality by declining to consent to a rule or by later withdrawing its consent. One effort in the realm of international humanitarian law to supplant the freedom principle with a form of natural law has been to use the Martens clause to overcome the hurdle of State non-consent. The clause in various iterations appears in a number of international humanitarian instruments. One of the most recent and prominent versions is set out in Article 1(2) of Additional Protocol I, which provides as follows: "In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from dictates of public conscience."[42] The argument is that the Martens clause, as customary international law, carves out an exception to the freedom principle by imposing limitations on States to which they have not consented.

---

41. *See* MICHAEL J. GLENNON, THE FOG OF LAW: PRAGMATISM, SECURITY, AND INTERNATIONAL LAW 17–18, 33, 64–65 (2010).

42. Additional Protocol I, *supra* note 17.

This argument is unconvincing. The clause is not a one-sentence cure-all that forever resolves all future legal ambiguities that might be created by technological innovation.[43] Assuming that the Martens clause does constitute customary international law[44]—which may not be the view of the United States[45]—it's doubtful whether States such as the United States have consented to that rule outside of specific treaties in which it exists,[46] and more doubtful still that the vague terms of the clause[47] necessarily have the

---

43. *See generally* David Friedman, *Does Technology Require New Law?*, 25 HARVARD JOURNAL OF LAW AND PUBLIC POLICY 71 (2001).

44. In its advisory opinion on the *Legality of the Threat or Use of Nuclear Weapons*, the ICJ said that the clause "had proved to be an effective means of addressing rapid evolution of military technology," 1996 I.C.J. 226, ¶ 78 (July 8), and that it represents customary international law. *Id.*, ¶ 84.

45. In 1987, the Deputy Legal Adviser of the U.S. State Department, Michael J. Matheson, identified those provisions of Additional Protocol I that the United States considers customary international law. Article 1(2) was not among them. *See* Michael J. Matheson, *The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AMERICAN UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLICY 419, 425 (1987). "No retreat from or disavowal of the Matheson announcement has been issued by any branch or department of the U.S. government." SOLIS, *supra* note 12, at 134 n.68. For an indication that the United States interprets the clause merely as recognition of the continued validity of customary rules that have not been modified by treaty, see BURRUS M. CARNAHAN, CUSTOMARY RULES OF INTERNATIONAL HUMANITARIAN LAW, REPORT ON THE PRACTICE OF THE UNITED STATES 6-2 (1997) (prepared for the International Committee of the Red Cross).

46. The United States has declined to ratify Additional Protocol I. Matheson, speaking in his official capacity, said as follows:

> First, the United States will consider itself legally bound by the rules contained in Protocol I only to the extent that they reflect customary international law, either now or as it may develop in the future. . . . Second, Protocol I now cannot serve in itself as the baseline for the establishment of common rules to govern the operations of military alliances in which United States forces participate. . . . Third, Protocol I cannot now be looked to by actual or potential adversaries of the United States or its allies as a definitive indication of the rules that United States forces will observe in the event of armed conflict and will expect its adversaries to observe. . . .

Matheson, *supra* note 45, at 420.

47. Guidance prepared by the U.S. Department of the Army for military lawyers indicated that the Martens clause "is difficult to apply in practice. Specific obligations resulting from the 'laws of humanity . . .' are extremely difficult to agree upon. . . . Such broad phrases in international law are in reality a reliance upon moral law and public opinion." U.S. DEPARTMENT OF THE ARMY, PAMPHLET NO. 27-161-2, 2 INTERNATIONAL LAW 15 (1962).

drastic effect of broadly negating the application of the freedom principle.[48] The United Kingdom argued as follows in *Nuclear Weapons*:

> While the Martens Clause makes clear that the absence of a specific treaty provision on the use of nuclear weapons is not, in itself, sufficient to establish that such weapons are capable of lawful use, the Clause does not, on its own, establish their illegality. The terms of the Martens Clause themselves make it necessary to point to a rule of customary international law which might outlaw the use of nuclear weapons. Since it is the existence of such a rule which is in question, reference to the Martens Clause adds little.[49]

The same would apply to cyber weapons: it's still necessary to point to an applicable rule, and a gap in the rules can exist. Nowhere in *Nuclear Weapons* does the ICJ suggest that the gap it identified is any less a gap because of the Martens clause. As the Court's opinion indicates, international law can *apply* to a given matter even though it contains a gap.[50]

None of this is to suggest that the international regime governing cyber operations is a blank slate. That the civilizing constraints of the law of war are not automatically eclipsed by technological innovation is the enduring reminder of the Martens clause. Clichéd but true, precepts of international law that have taken shape over centuries are the received wisdom of the

48. The Court had a chance to say that, if it had wanted to, in the *Nuclear Weapons* advisory opinion, *supra* note 35, and was in effect invited by the General Assembly to revisit the *Lotus* decision, but it declined to do so. Waldemar Solf suggested that the meaning of the principles of humanity and dictates of public conscience referred to in the clause "must be accepted in the practice of the states," suggesting that the clause—like any other treaty provision—has the effect of merely continuing in force pre-existing norms of customary international law that are not rendered inoperable by the treaty's application. *Remarks of Professor Waldemar Solf*, 2 AMERICAN UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLICY 481, 483 (1987).

49. Letter Dated 16 June 1995 from the Legal Adviser to the Foreign and Commonwealth Office of the United Kingdom of Great Britain and Northern Ireland, Together with Written Comments of the United Kingdom 48, filed in Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion (June 16, 1995), *available at* http://www.icj-cij.org/docket/files/95/8802.pdf.

50. Broad inapplicability, however, might merely be thought of as a broader gap; both connote ineffectuality but in different degrees. The notion of a law that applies but has no effect was famously derided by Anatole France. "The law," he wrote, "in its majestic equality, forbids the rich as well as the poor to sleep under bridges, to beg in the streets, and to steal bread." ANATOLE FRANCE, THE RED LILY 95 (LE LYS ROUGE) (Winifred Stephens trans., 1927) (1894).

ages, to be ignored by the digitally distracted at their peril. That international law does not unequivocally proscribe unleashing a computer virus to destroy centrifuges by changing the rotational speed of their motors[51] does not mean that it is irretrievably vague about using malware to bring down a civilian airliner by freezing its computerized avionics.

Nor do I proffer any new answer to the dilemma of when law interpreting begins and lawmaking ends, about how the needs of the present ought to be reconciled with the commands of the past, about when the impulses of the living ought to defer to the designs of the dead. We are still, to paraphrase Martin Amis, dozens of Henkins away from answers to those questions. I do suggest that the old lawyers' saying—*Le mort saisit le vif,* the dead grip the living—has it backward: the living grip the dead, in my view, not because they must but because holding fast to settled solutions is the best way to give law the predictability and stability it requires, to nail down what we regard as progress, and simply to save ourselves work. The urge to loosen that grip grows stronger with every "next big thing" in warfighting technology, however: "it is never enough to claim a country; it must be held. It must be held and made secure, every generation."[52] The claim that the law doesn't reach *their* conduct will forever be made by scofflaws seeking to evade its reach. That claim is no less repugnant in the realm of cyber rules than elsewhere—but in cyber rules, as elsewhere, that claim must be considered, for in no realm can either lawgivers or law interpreters evade the command of the law to decide what the rules cover and what they do not. The response to a spurious assertion of a gap, therefore, is not to profess that gaps do not exist; the response is to assess whether a particular gap *does* exist and, if not, to enforce the law.

The point, then, is that there *is* a difference between lawmaking and law interpreting; that however hard it is to disentangle the two, it's *possible* that gaps in the law governing cyber conflict can exist; and that given that possibility, classification choices that often have been assumed to present neat dyads in fact present triads. Realistic choices, in international law as else-

---

51. The State Department Legal Adviser appears to have implied that Olympic Games constituted a use of force because the physical consequences of the attack worked the same kind of physical damage that dropping a bomb or firing a missile would have. *See* Koh, *supra* note 21. "*Cyber activities*," he added, "*that proximately result in death, injury, or significant destruction would likely be viewed as a use of force*." *Id.* (emphasis in original). Why *proximate* causation is required is not clear; under traditional analysis, kinetic activity that is the cause-in-fact of death, injury or significant destruction would likely be viewed as a use of force.

52. HILLARY MANTEL, WOLF HALL 255 (2009).

where, entail more than mechanical, on/off, light-switch classification. Realistic lawyers are skeptical of essentialist and foundationalist value claims.[53] Realistic lawyering reflects the genealogy of legal rules, the consequences of one interpretation versus another, the structure of incentives and disincentives that a given interpretation would yield, the political and historical context in which a legal issue arises, the expectations of the parties, the level of compliance that rules actually generate, and a variety of other matters none of which can be captured in neat interpretive algorithms as part of a robotic exercise of categorization. Formalism leaves policymakers scratching their heads in puzzlement when pretended "outcomes" don't actually flow from the forms, from the categories, from the rigorous syllogisms that formalist lawyers lay out for them; exclusive reliance upon the categories masks the real factors on which outcomes inevitably depend. A broader approach, which some have called pragmatism,[54] doesn't purport to be certain, universalist or complete. It acknowledges the law's inevitable indeterminacy and inability to foresee, let alone resolve, every possible future case. It recognizes the inconvenient truth "that existing legal rules themselves can be understood only in the light of ideas and information drawn from outside law. . . ."[55] It accepts the risk of phony assertions of gaps in the law as the price of keeping the law honest, alive and understandable. It counsels against reliance upon past choices that are wrongly claimed to have eliminated the need for future choices.[56] But it does identify, or at least tries to identify, what's really at stake in legal disputes, whether old categories are up to the task of resolving those disputes, and where new categories might be needed. And it doesn't stifle legal reform with specious claims of systemic completeness.

III. THE IMPROBABILITY OF NEW LIMITS

A better way of posing the question that I now proceed to address, therefore, is not "whether gaps in the international rules governing cyber con-

53. GLENNON, *supra* note 41, at 5.

54. For a contemporary version in this context, see *id.* For an earlier, and prescient, exploration of some of the same themes, see SAMUEL VON PUFENDORF, ON THE DUTY OF MAN AND CITIZEN ACCORDING TO NATURAL LAW 108 (James Tully ed., Michael Silverthorne trans., 1991) (1682).

55. Dickinson, *supra* note 1, at 122.

56. *Cf.* HART, *supra* note 28, at 129.

flicts are likely to be filled"; rather, the question is whether States are likely to consent to new law that limits their freedom to use cyber weapons.

Law is a form of cooperation. Certain conditions normally exist when cooperative mechanisms like law emerge and function properly.[57] Actors within the system, for example, are relatively equal. Future dealings are expected. Trust is high. A consensus exists concerning foundational values. The cost of non-cooperation is high. Individual and collective interests align. Underlying social norms reinforce legal norms. Free riders and transgressors are easily spotted and penalized.

For better or worse, however, these and other conditions necessary to promote the emergence and development of legalist constraints are not present in sufficient degree to support further international rules governing cyber conflict—any more than those conditions have been present, in the past, to support the emergence of rules governing clandestine or covert intelligence operations of which cyber activity normally is a part.

When States are equal in capability, the imposition of legal limits freezes in no advantage or disadvantage. Because cyber capabilities are concealed, however, relative capability becomes speculative, leaving States without the ability to evaluate beforehand the apparent advantages and disadvantages that new rules might reify.[58] States will not regulate the pursuit of core security interests based upon speculation (hence the muted international enthusiasm for Russia's proposal for an international cyber weapons

57. Andrew Hurrell has noted that "fundamental differences in religion, social organization, culture and moral outlook . . . may block or, at least, complicate cooperative action." Andrew Hurrell, *Power, Institutions, and the Production of Inequality*, *in* POWER IN GLOBAL GOVERNANCE 33, 36 (Michael Barnett & Raymond Duvall eds., 2005). *See generally* Simon Maxwell, *Why Cooperate?* (paper distributed at Reforming the United Nations Once and for All, World Economic Forum, Davos, Switzerland (Jan. 23, 2004)) (on file with author); Sarah Gillinson, *Why Cooperate? A Multi-Disciplinary Study of Collective Action* (Overseas Development Institute, Working Paper No. 234, 2004), *available at* http://www.odi.org.uk/resources/docs/2472.pdf. Seminal works in this area include COOPERATION UNDER ANARCHY (Kenneth A. Oye ed., 1986); ROBERT AXELROD, THE EVOLUTION OF COOPERATION (1984); and ROBERT O. KEOHANE, AFTER HEGEMONY: COOPERATION AND DISCORD IN THE WORLD POLITICAL ECONOMY (1984).

58. For similar analysis see Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, *in* FUTURE CHALLENGES IN NATIONAL SECURITY AND LAW 6 (Peter Berkowitz ed., 2011), *available at* http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf ("Offensive cyber weapons are guarded secrets because knowledge about the weapon enables the building of defenses and because revelation about attack capabilities would reveal a lot about exploitation capabilities."). *See also* Jack Goldsmith, *The New Vulnerability*, NEW REPUBLIC, June 7, 2010, at 21.

ban).[59] For similar reasons, customary international rules on these issues are unlikely. Customary international law depends upon connecting dots of historical precedents that form patterns of practice, but States have been disinclined to talk publicly about cyber incidents in which they have been involved.

When future dealings are expected, States confront a greater incentive to come up with a mutually advantageous rule, such as the UN Charter's prohibition against non-defensive use of force. If, however, the sponsor of a cyber attack can't be identified because sponsorship of the attack—or the attack itself—is concealed, as is often true of cyber attacks, then the future casts no shadow and no State need be concerned about future rewards or penalties; law can impose no punishment.

More than anything else, however, it is this element of attributability—the reciprocal ability to say "who did it"—that makes law work. When a transgressor can be identified, penalties can be assessed, and retaliation and deterrence are possible—and so is legal regulation. Attribution permits the target to assign responsibility. It provides the rules' ultimate enforcement mechanism—the ever-present threat of retaliation and punishment. It therefore establishes compliance incentives. And attributability enables legal recourse against transgressors, not only in the International Criminal Court and other international tribunals, but also in the domestic courts of nations that comply with their international obligation to investigate and prosecute war crimes. If cyber activity and its sponsor are concealed, however, and verification of compliance is impossible, so too is deterrence[60] and effective legal regulation. No verifiable international agreement can regulate the covert writing or storage of computer code useful for launching a clandestine cyber attack.

Indeed, this single reciprocal condition—the ability of a target nation to identify and threaten assailants in one way or another—underpins the entire

---

59. *See* U.N. GAOR, Letter dated September 23, 1998 from the Permanent Representative of the Russian Federation to the United Nations to the Secretary General concerning Agenda Item 63, U.N. Doc. A/C.1/53/3 (Sept. 30, 1998).

60. For commentary on deterrence in cyber conflict, see Patrick M. Morgan, *Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm*, *in* COMMITTEE ON DETERRING CYBERATTACKS, NATIONAL RESEARCH COUNCIL, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 55 (2010), *available at* http://www.nap.edu/openbook.php?record_id=12997&page=55; Mike McConnell, *To win the cyber-war, look to the Cold War*, WASHINGTON POST, Feb. 28, 2010, at B1.

legal edifice that regulates armed conflict.[61] The prohibition against aggression is empty absent an ability to ascertain the aggressor. The protection of noncombatants disappears unless the assailant is identifiable. The law of neutrality is meaningless absent an ability to identify a belligerent. The possibility of reprisal or self-defense evaporates absent an ability to know what nation to take measures against. The notion of command responsibility dissolves absent knowledge of who the commander is. In marginal instances States' interests induce compliance with the law of war despite attribution difficulties; compliance sometimes can produce extrinsic benefits for the law-abiding, such as shortening conflicts or stabilizing post-conflict environments even when adversaries flout the law of war. But the modern rules of war are effectively premised on attributability.

Internationally, the reciprocal possibility of identification thus makes violence less likely because it exposes the attacker to risk in three ways. First, retaliation is possible. While the modern laws of war generally prohibit reciprocal violation, in practice the vitality of those rules often has depended upon the threat of retaliation. It would not, for example, have been permissible under international law to use chemical weapons against Nazi Germany in response to its putative use of such weapons, but it is entirely plausible that Hitler exercised restraint because of the credible threat to do so by Roosevelt and Churchill.[62] Second, the identification of transgressors makes remedial legal action possible. For States, penalties for charges of aggression or disproportionate and indiscriminate attacks, for example, can take the form of economic sanctions, reparations or other remedies, as Iraq discovered following its invasion of Kuwait.[63] For individuals, acts perpetrated during periods of armed conflict that transgress the laws of war, such as targeting civilians or torturing adversaries, give rise

---

61. *See* James D. Murrow, *When Do States Follow the Laws of War?*, 101 AMERICAN POLITICAL SCIENCE REVIEW 559, 560 (2007) (describing the role of "reciprocal enforcement" in "[c]ompliance with the laws of war").

62. President Franklin D. Roosevelt warned that any use of poisonous or noxious gases by the enemy would be met by the "fullest possible retaliation":

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

Use of Poison Gas, 8 DEPARTMENT OF STATE BULLETIN 507 (1943).

63. *See* S.C. Res. 661, U.N. Doc. S/RES/661 (Aug. 6, 1990).

to individual criminal responsibility. The war crimes against Bosnian Croat and Muslim civilians during the Bosnian war of the 1990s could not be prosecuted had the alleged perpetrators, such as Radovan Karadžić and Ratko Mladić, not been identified and indicted. Third, identification can impose reputational costs that are not without consequences. More than one prominent American official has escaped formal punishment for the mistreatment of prisoners in recent years but endured widespread denunciation because the chain of command was (at least on occasion) transparent enough to pinpoint responsibility.

Sometimes, of course, those costs are light enough or improbable enough for a transgressor to absorb painlessly. Muammar Gaddafi flouted all legal obligations in his effort to remain in power in Libya, and Syrian President Bashar al-Assad, while attempting to exonerate himself of personal liability, has long seemed undeterred by the possibility of criminal prosecution for crimes against his country's civilians. An effective rule of law ultimately relies on making the costs of non-compliance exceed the costs of compliance; the history of international law has been a struggle to do just that. Anonymity makes violation cost-free, however, because the assignment of responsibility and imposition of penalties are impossible. Attributability, in contrast, creates reciprocity-induced restraints. It produces greater regularity in conflict management, enhanced predictability in inter-State relations and increased systemic stability.

How, then, do the conditions needed for effective international rules affect the amenability of cyber operations to international regulation of cyber weapons and cyber attacks? Cyber operations' "attribution problem,"[64] so-called, in reality exists at three levels. To attribute a cyber attack to a State, it's necessary to establish what computer was used, who was sitting at the computer (if it's not government-owned), and what government or organization that person worked for. Sophisticated cyber attacks of the sort launched by governments normally are extremely difficult to trace at any of those levels. Most experts believe that the possibility of concealment is baked into the structure of the Internet and cannot feasibly be eliminat-

64. *See* Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARVARD INTERNATIONAL LAW JOURNAL 373, 397–408 (2011). For an excellent review of the technological difficulties involved in attribution with regard to cyber operations, see also JOEL BRENNER, AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE 50–51, 133–34, 234–35 (2011); David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARVARD NATIONAL SECURITY JOURNAL 531 (2011).

ed.[65] Circumstantial evidence and inferred motives have led experts to suspect State involvement in a number of cyber attacks over recent years, but have not provided the level of probability long thought necessary to justify military retaliation.

It remains likely, therefore, that the law of war, compliance with which depends heavily upon attributability and related background conditions, will not be refined to further regulate cyber operations.

The possibility of further regulation cannot be dismissed, however, particularly after the *New York Times* confirmed that the United States and Israel were behind Stuxnet.[66] Policymakers cannot automatically assume deniability, for secrecy is not the only incentive that drives States. Policymakers confront a dilemma: they seek secrecy, of course, for all the reasons that plausible deniability is sought in covert operations; "[n]on-attribution to the United States for covert operations," the Church Committee found, "was the original and principal purpose of the so-called doctrine of 'plausible denial.'"[67] But policymakers at the same time want the world—and often need the world—to know of their successes. They are credit-seeking, blame-avoiding actors. They seek praise for what they do. They don't want to be found at fault if the public in the fullness of time learns that war might have been avoided through the discrete use of some amazing new application like Stuxnet. They want to make their political leaders look tough, their software designers look smart and their nation's adversaries look twice before attacking. All this requires public disclosure—leaks.[68] Attribution, therefore, cannot be masked entirely by computer technology, even if the Internet does remain opaque. No "HAL 9000" runs the

65. *See* Clark & Landau, *supra* note 64, at 531 ("The Internet was not designed with the goal of deterrence in mind. . . ."); *see also* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 JOURNAL OF CRIMINAL LAW AND CRIMINOLOGY 379 (2007) (discussing how computing technology complicates attribution); W. Earl Boerbert, *A Survey of Challenges in Attribution*, *in* COMMITTEE ON DETERRING CYBERATTACKS, *supra* note 60, at 41, 41–52, *available at* http://www.nap.edu/openbook.php?record_id=12997&page=41 (outlining the barriers to both technological and human attribution in cyberspace).

66. *See* Sanger, *supra* note 3.

67. SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, INTERIM REPORT: ALLEGED ASSASSINATION PLOTS INVOLVING FOREIGN LEADERS, S. REP. NO. 94-465, at 11 (1975), *available at* http://www.intelligence.senate.gov/pdfs94th/94465.pdf.

68. "That's another of those irregular verbs, isn't it? I give confidential press briefings; you leak; he's being charged under section 2A of the Official Secrets Act." *Yes, Prime Minister: Man Overboard* (BBC television broadcast Dec. 3, 1987).

show—yet—and human involvement is a trapdoor, waiting to be exploited by spies and reporters.

That being true, what lies ahead? The answer depends largely upon the course of future events. At one end of the spectrum lies an overt, immediately attributable cataclysmic cyber shock—a "digital Pearl Harbor" involving, say, a massive, sustained East Coast power outage in midwinter, breaking pipes and disabling ATMs, police communications and air traffic control systems. In that event, pressure would be brought to bear on the U.S. government to take the lead in devising new international rules to prevent a recurrence, much as occurred in 1919 at Versailles and 1945 in San Francisco. At a minimum, new rules could take the form of targeted, universal sanctions directed at wrongdoers; at a maximum one could envision an explicit redefinition of self-defense to permit the use of kinetic force in response to a cyber attack.

At the other end of the spectrum lie "drip-drip" clandestine cyber attacks—an occasional "flash crash" on a stock exchange that no one can explain, a mysterious airline accident here, a strange power blackout there, incidents extending over months or years, with no traceable sponsorship. Although the ultimate cost of these attacks could be great, they are likely to be tolerated because the costs are incurred gradually and incrementally, because no sponsor can be quickly identified[69] and because the countervailing benefits of cyber weapons seem greater by comparison (as with Stuxnet). For a financially strapped and war-weary public and an American military establishment inclined toward "light footprints," those are strong reasons not to bargain away cyber weapons.

In this scenario, cyber weapons research is driven not by adversaries' actual capabilities but by the reciprocal assumption that if we can discover it, an adversary can also discover it—the classic security dilemma that creates an inexorable forward momentum. Cyber operations are in this view

69. As the time required to identify an attacker increases, the likelihood of a forceful response decreases. The Libyan bombing of Pan Am Flight 103 is an example. Confirming the Libyan government's involvement took years, during which the aggrieved States relied upon law enforcement rather than military remedies. Immediate confirmation might have drawn comparisons to the German sinking of the *Lusitania* in 1915, which contributed significantly to U.S. entry into World War I. *See* Jonathan B. Schwartz, *Dealing with a "Rogue State": The Libya Precedent*, 101 AMERICAN JOURNAL OF INTERNATIONAL LAW 553, 555–56 (2007) (describing how the United States and United Kingdom "elected to treat the bombing of Pan Am 103 as a crime under their domestic legal processes" rather than "consider[ing] [it] an 'act of war,' as the United States had treated the Libyan-sponsored attack on off-duty U.S. military personnel at a Berlin nightclub . . . in 1986").

regarded as merely the latest efforts—the latest *successes*—at injecting less risk into combat, merely the most recent in a long history of efforts by States to fight at a greater distance, to afford greater protection to non-combatants (and combatants), to enhance proportionality—in effect, to pursue many of the ends of humanitarian law. States in this scenario will continue to seek concealment but will recognize that the operation is discoverable and attributable. In the recognition of that risk lies the possibility of some international legal regulation. But that regulation, if it occurs, will not likely be deep or broad, because it will be limited by the same incentive structure that drives it: policymakers will continue to seek out rules, here as elsewhere, intended to permit what they're doing but to limit what their adversaries might do. So the blades of such rules are likely to be dull, for the authors' own protection.

How likely is each of those scenarios? The truth is that only a handful of people in the world—if that—are knowledgeable enough to say. I am not one of them. It would be a mistake, however, to underestimate the humanitarian and institutional costs lurking in the seemingly benign, second scenario of drip-drip attacks and counterattacks. If they have anything in common with warriors of the past, cyber warriors will be less inhibited in initiating computer-induced violence. Anonymity, and the distance from violence that provides it, will afford not only safety and insulation against retaliation; distance removes inhibitions against committing acts of violence. Cyber and drone technologies insert greater separation between hunter and victim than ever before: no screams are audible and no blood is visible when pain is inflicted thousands of miles away, merely by hitting the "enter" button on a keyboard.[70] The hunter may not even know whether a "kill" has occurred. In a sequence of relentless cyber attacks and counterattacks, the risk assessment of warfighting is carried out behind closed doors, in the security of Sensitive Compartmented Information Facilities, safely

70. Joshua Greene's research has shown that the thought of killing with one's bare hands is more disagreeable than the thought of killing by throwing a switch that kills from afar. Primates find screams of pain aversive. *See* Joshua D. Greene, *The Secret Joke of Kant's Soul*, *in* 3 MORAL PSYCHOLOGY: THE NEUROSCIENCE OF MORALITY: EMOTION, BRAIN DISORDERS, AND DEVELOPMENT 35, 43 (Walter Sinnott-Armstrong ed., 2008) ("[W]hen harmful actions are sufficiently impersonal, they fail to push our emotional buttons, despite their seriousness, and as a result we think about them in a more detached, actuarial fashion."). For the philosophical origins of the "trolley problem," see Judith Jarvis Thomson, *The Trolley Problem*, 94 YALE LAW JOURNAL 1395 (1985); Philippa Foot, *The Problem of Abortion and Negative and Positive Duty: A Reply to James LeRoy Smith*, 3 JOURNAL OF MEDICINE AND PHILOSOPHY 253 (1978).

immune from legislative or public scrutiny. Cyber attacks, as "sources and methods," are kept secret from Congress. No citizenry is aroused to object. Indeed, the public doesn't even know that an attack has been launched. Which States or terrorists are behind the attacks are—in the public sphere—anyone's guess. Retaliatory attacks, as well as preventive and preemptive attacks, are launched instantaneously, and are thus triggered by an adversary's presumed capability and inferred motives rather than by actual or apparent provocations. As a result, drip-drip strikes—and something very like war—occur more often, in more places, against more targets, based upon weaker evidence.

If that's the road ahead, gaps or no gaps, we are in for a rough ride.