The Dark Future of International Cybersecurity Regulation

Michael J. Glennon*

States are not likely to consent to new international rules that restrict the use of cyber weapons.

Law is a form of cooperation. Certain conditions normally exist when cooperative mechanisms like law emerge and function properly.[1] 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 possessed of equal military capabilities, the imposition of legal limits cannot by definition freeze in an 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.[2] 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

---

* Professor of International Law, Fletcher School of Law and Diplomacy, Tufts University. 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, and Gary Solis for comments on an earlier draft. Errors and views are mine.

1. 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 35, 36 (Michael Barnett & Raymond Duvall eds., 2005); *see also* Simon Maxwell, Why Cooperate? (2004) (paper distributed at forum, Reforming the United Nations Once and for All, World Economic Forum, Davos, Switzerland) (on file with author); Sarah Gillinson, *Why Cooperate? A Multi-Disciplinary Study of Collective Action* (Overseas Dev. Inst.,Working Paper No. 234, 2004), *available at* http://www.odi.org.uk/resources/docs/2472.pdf; *see generally* Cooperation Under Anarchy (Kenneth A. Oye ed., 1986); Robert Axelrod, The Evolution of Cooperation (1984); Robert O. Keohane, After Hegemony: Cooperation and Discord in the World Political Economy (1984).

2. For an argument along similar lines 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."); s*ee also* Jack Goldsmith, *The New Vulnerability*, New Republic, June 7, 2010, at 21.

weapons ban).[3] 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.[4]

When future dealings are expected, states confront a greater incentive to come up with a mutually advantageous rule, such as the U.N. Charter's prohibition against non-defensive use of force.[5] 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[6] 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 legal edifice that regulates armed conflict.[7] 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

---

3. *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).

4. *See, e.g.*, Scott Shane, *Cyberwarfare Emerges from Shadows for Public Discussion by U.S. Officials*, N.Y. TIMES, Sept. 27, 2012, at A10. ("For years, even as the United States carried out sophisticated cyberattacks on Iran's nuclear program and the Pentagon created a Cyber Command, officials have been hesitant to discuss American offensive cyberwarfare programs openly.").

5. *See* U.N. Charter art. 2, para. 4.

6. For commentary on deterrence in cyber conflict, see Patrick M. Morgan, *Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm*, *in* NATIONAL ACADEMY OF SCIENCES, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 55 (2010); Mike McConnell, *To Win the Cyber-War, Look to the Cold War*, WASH. POST, Feb. 28, 2010, at B1.

7. *See* James D. Morrow, *When Do States Follow the Laws of War?* 101 AM. POL. SCI. REV. 559, 560 (2007) (describing the role of "reciprocal enforcement" in "[c]ompliance with the laws of war").

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.[8] 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.[9] Second, the identification of transgressors makes remedial legal action possible. For states, penalties for unlawful 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.[10] For individuals, acts perpetrated during periods of armed conflict that transgress the laws of war, such as targeting civilians or torturing adversaries, give rise to individual criminal responsibility. The war crimes against Bosnian and Croat 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.[11] Third, identification can impose reputational costs that

---

8. Compliance with international law, of course, can occur for countless reasons; State Department Legal Adviser Harold Koh once noted that "[l]ike most laws, international rules are rarely enforced, but usually obeyed." Harold Hongju Koh, *Why Do Nations Obey International Law?*,106 YALE L.J. 2599, 2603 (1997). For an analysis of the benefits states can garner from voluntarily following the law of war, see Robert D. Sloane, *Prologue to a Voluntarist War Convention*, 106 MICH. L. REV. 443, 451 (2007) (advocating for a non-reciprocal "voluntarist war convention," while rejecting the view "that no benefits accrue to the party that follows the convention" simply because it is not reciprocal).

9. 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 DEP'T STATE BULL. 507 (1943).

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

11. Karadžić was apprehended in July 2008 and his trial is still ongoing. *See* Marlise Simons, *Former Bosnian Leader Begins His Defense at Genocide Trial*, N.Y. TIMES, Oct. 17, 2012, at A8.

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 transparent enough to pinpoint responsibility.[12]

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.[13] 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 interstate 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,"[14] so-called, in

---

Mladić was apprehended in May 2011 and his trial is also ongoing. *See* Marlise Simons, *The Hague: Mladic's Trial Resumes*, N.Y.TIMES, July 9, 2012, at A8.

12. *See, e.g.*, Jordan J. Paust, *Civil Liability of Bush, Cheney, et al. for Torture, Cruel, Inhuman, and Degrading Treatment and Forced Disappearance*, 42 CASE W. RES. J. INT'L L. 359, 359 (2009) ("It is well beyond reasonable doubt that during an admitted 'program' of serial criminality designed to use secret detention and coercive interrogation of human beings from the waning months of 2001 until 2009, former President Bush, former Vice President Cheney, Alberto Gonzales, and several other members of the Bush Administration authorized, ordered, and/or abetted the forced disappearance of persons [and] other war crimes . . . including torture [and] cruel, inhuman, and degrading treatment of human beings . . . ."); Diane Marie Amann, *Abu Ghraib*, 153 U. PA . L. REV. 2085, 2086 (2005) (describing how in the aftermath of the Abu Ghraib scandal, "[a] few soldiers were prosecuted for detainee abuse, but generals implicated in government reports were not, and high-ranking civilians won promotion").

13. *See generally* Michael W. Doyle & Geoffrey S. Carlson, *Silence of the Laws? Conceptions of International Relations and International Law in Hobbes, Kant, and Locke*, 46 COLUM. J. TRANSNAT'L L. 648, 655 (2008) ("The key message of Hobbesian Realism is that law is weak, but relevant. Any law that reflects the material, prestige, or security interests of a state would be complied with. Moreover, even when those interests dictate defection, states will be reluctant to acquire the reputation of faithlessness when they rely on cooperation for survival (citing THOMAS HOBBES, LEVIATHAN 115 (Michael Oakeshott ed., Collier 1962) (1651)); *see also* Andrew Hurrell, *International Society and the Study of Regimes: A Reflective Approach*, *in* REGIME THEORY AND INTERNATIONAL RELATIONS 56 (Volker Rittberger ed., 1993) ("The core claim is that regimes are created and that states obey the rules embodied in them because of the functional benefits that they provide."); LOUIS HENKIN, HOW NATIONS BEHAVE 47 (1968) (observing that "nations will observe international obligations unless violation promises an important balance of advantage over cost").

14. *See* Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 397-408 (2011). For an excellent review of the technological difficulties involved in attribution with regard to cyber operations, see 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 HARV. NAT'L SEC. J. 531 (2011).

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 eliminated.[15] 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.[16] 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. '"[17] 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.[18] They don't want to be found at fault if the public in the fullness of time comes to learn that war might have been avoided through the discrete

15. *See* Clark & Landau, *supra* note 14, 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 J. CRIM. L. & CRIMINOLOGY 379 (2007) (discussing how computing technology complicates attribution); W. Earl Boerbert, *A Survey of Challenges in Attribution*, *in* COMM. ON DETERRING CYBERATTACKS, NAT'L RESEARCH COUNCIL, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 41, 41-52 (2010), *available at* http://www.nap.edu/openbook.php?record_id=12997&page=41 (outlining the barriers to both technological and human attribution in cyberspace).

16. *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1.

17. SELECT COMM. 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.

18. A brief glance at recent political history bears out this observation. *See* Scott Wilson, *Bin Laden Raid Now a Flash Point on Trail*, WASH. POST, May 1, 2012, at A4 ("President Obama has placed the killing of Osama bin Laden at the center of his reelection effort in a way that is drawing criticism for turning what he once described as an American victory into a partisan political asset."); Dan Froomkin, *Four Years After 'Mission Accomplished,'* WASHINGTONPOST.COM (May 1, 2007), http://www.washingtonpost.com/wp-dyn/content/blog/2007/05/01/BL2007050100936.html ("Four years ago today, Bush flew aboard the USS Abraham Lincoln aircraft carrier in 'Top Gun' style, stood under a banner proclaiming 'Mission Accomplished,' and proudly declared: 'Major combat operations in Iraq have ended. In the battle of Iraq, the United States and our allies have prevailed.'").

use of some amazing new app like Stuxnet. They want to make their nations' political leaders look tough, their software designers look smart, and their nation's adversaries look twice before attacking. All this requires public disclosure, which typically occurs through leaks.[19] Attribution, therefore, cannot be masked entirely by computer technology, even if the Internet does remain opaque. No "HAL 9000" runs the show – yet – and human involvement is a trapdoor, waiting to be exploited by spies and reporters.[20]

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 mid-winter, breaking pipes and disabling ATM machines, 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,[21] 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

19. "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." JONATHAN LYNN & ANTONY JAY, THE COMPLETE YES MINISTER ("Man Overboard") (1984).

20. Independent experts have also attributed some attacks. For example, Stuxnet was discovered by anti-virus companies, named by a Microsoft technician, and was later decoded and analyzed by a world-wide group of computer security specialists. The connection between Stuxnet and the failing centrifuges in Iran was first made by an industrial control system expert in Hamburg and only later picked up by the Western media. *See* Michael Joseph Gross, *A Declaration of Cyber-Warfare*, VANITY FAIR, Apr. 2011, at 152.

21. 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 one 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 AM. J. INT'L L. 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").

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 can in this view be 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.[22] 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 pretty 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 counter-attacks. 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.[23] The hunter may not even know whether a "kill" has ever occurred. In a sequence of relentless cyber attacks and counter-attacks, the risk assessment of war-fighting is carried out behind closed

---

22. *See, e.g.*, Duncan Blake & Joseph S. Imburgia, *"Bloodless Weapons"? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining them as "Weapons,"* 66 A.F. L. REV. 157, 161 n.7 (2010) ("The 2007 cyber attacks against Estonia and the 2008 cyber attacks against Georgia demonstrate how cyber warfare can be used against a country to influence that country's actions without causing widespread human injury or death.").

23. 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 L.J. 1395 (1985); Philippa Foot, *The Problem of Abortion and Negative and Positive Duty: A Reply to James LeRoy Smith*, 3 J. MED. & PHIL. 253 (1978).

doors, in the security of Sensitive Compartmented Information Facilities (SCIFs), safely immune from legislative or public scrutiny.[24] Cyber attacks, as "sources and methods," are kept secret from Congress.[25] 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 is – in the public sphere – anyone's guess. Retaliatory attacks, as well as preventive and preemptive attacks, 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, we are in for a rough ride.

24. *See* Andru E. Wall, *Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action*, 3 HARV. NAT'L SEC. J. 85, 92 (2011) (describing how "cyberwarfare" is "conducted in secret and in environments where public acknowledgement of the U.S. military's involvement may raise diplomatic and national security concerns").

25. *See* Vicki Divoll, *The "Full Access Doctrine": Congress's Constitutional Entitlement to National Security Information from the Executive*, 34 HARV. J.L. & PUB. POL'Y 493, 522 n.104 (2011) (describing the National Security Act's broad "sources and methods" exception to the intelligence community's obligation to keep Congress "fully and currently informed").